A Methodology to Protect MANET Against Application Layer DDoS Attacks

Synopsis of the PhD Thesis

Submitted by

Mr. Kiran Madhukar Salunke

(Roll No: P009)

Department of Electronics and Telecommunication Engineering

Supervisor

Dr. Suresh Kurumbanshi

Submitted in partial fulfilment of the requirements of

DOCTOR OF PHILOSOPHY (Engineering)

MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING
SVKM's NARSEE MONJEE INSTITUTE OF MANAGEMENT STUDIES (Declared as Deemed-to-be University Under Section 3 of the UGC Act, 1956)
V. L. Mehta Road, Vile Parle (West)
MUMBAI –400056

2025

TABLE OF CONTENTS

SECTION NO.	TITLE	PAGE NO.
	Abstract	3
1	Introduction	4
2	Literature review	7
	2.1 Detection of Application Layer DDoS Attacks in MANET	9
	2.2 Mitigation and Feature Optimization in MANET Intrusion Detection	9
	2.3 Flash Crowd Differentiation and Unified Framework Approaches	9
	2.4 Research Gaps Identified	12
3	Objectives	13
4	Contribution	15
	4.1 Optimized Detection of Application Layer DDoS Attacks in MANET Using Traffic Analysis	16
	4.2 Optimized Mitigation Using Feature Selection in Resource-Limited MANET Nodes	18
	4.3 Flash Event Differentiation Using Information Divergence	23
	4.4 SHIELD Framework with Optimized Routing and QoS Preservation	27
5	Results and discussion	29
	5.1 Classification of Benign and Malicious Traffic	29
	5.2 Optimized selection of features via BM-HHO	31
	5.3 Load Balancing analysis via I-CMIWO	32
	5.4 PCC-based differentiation of application layer DDoS attack and Flash Events.	34
	5.5 QoS Parameters analysis during and after DDoS Attack	34
	5.6 MANET adaptability analysis.	35
	5.7 Unified SHIELD framework	36
	5.8 SHIELD Evaluation on CIC-DDOS-2019 Dataset	37
	5.9 SHIELD Evaluation on EDGE IIoT Dataset	37
	5.10 Hardware Deployment of SHIELD Methodology	38
6	Conclusion	40
7	Future scope	41
8	Publications	42
	References	43

Abstract

Mobile-Ad-Hoc Networks (MANETs) experience growing Distributed Denial of Service (DDoS) attacks at the application layer because of their decentralized structure, which is joined with inadequate node assets, generates striking targets for attackers. The attacks masquerade as normal user activities and flash events to create performance disruptions by overwhelming nodes and blocking service availability. This study introduces the adaptive SHIELD defense methodology, which combines detection capabilities with mitigation features and traffic classification and intelligent routing to boost MANET resilience while maintaining Quality of Service (QoS). The proposed system uses a Xavier-initialized SoftPlus Convolutional Neural Network (XSP-CNN) for high-precision real-time detection of application-layer attacks, which reaches 98.96 % classification accuracy. The Proposed mitigation strategy slips the Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) to optimize feature selection at reduction in the computational costs. The statistical model that is developed based on Pearson metric can distinguish between flash events and benign flooding with a classification accuracy of 99.8 %. SHIELD is system-level integrated with adaptive load balancing implementation, which is Interpolation-based Crossover-Mutation Invasive Weed Optimization (I-CMIWO), and a lightweight Double Shift Right Complement (DSRC) filtering scheme. In this architecture, the suggested system conducts automatic load distribution and purposeful transmissions of packets and real-time removal of threats to mobile systems under the various types of nodes. The proposed system has high true positive rates and low false alarm rates of below 1.2 %. The infrastructure maintains QoS integrity during attack situations through a performance gain of up to 40 percent improvement versus no defense in attacks. The paper focuses on concerning security loopholes in MANETs by a lightweight and scalable validated solution which can provide real-time response to intrusions and can differentiate flash events. The SHIELD framework provides a resilient base for future autonomous MANET defense systems through experimental validation and architectural integration, and design reproducibility. The research compares SHIELD to current MANET DDoS defense systems which shows that SHIELD provides better protection through its application-layer defense and its ability to manage sudden traffic surges and its hybrid optimization approach. SHIELD demonstrated strong performance against an attack generated by the LOIC tool and achieved detection accuracy as high as 99.51 % in a hardware experiment. SHIELD provides a deployable defense system which protects mobile wireless networks from security threats through its combination of real-time intelligent detection with adaptive resource-aware mitigation and accurate flash attack differentiation and resilient routing. The research develops MANET security standards which enable distributed protection systems for upcoming wireless communication networks.

1. Introduction

Mobile-Ad-Hoc Networks (MANETs) serve as a fundamental communication paradigm in modern wireless systems because they operate without infrastructure while organizing themselves and handling changing network topologies. MANETs function well in mission-critical situations, including disaster recovery and battlefield communication and vehicular networks and remote sensing, because they do not requisite centralized infrastructure. MANETs demonstrate litheness, however they come across major security challenges. The decentralized structure of MANETs, along with their open wireless medium and self-governing nodes, makes them highly susceptible to Distributed Denial-of-Service (DDoS) attacks, as illustrated in Figure 1. Application-layer DDoS attacks signify a particularly hazardous type of attack amid others. The attacks differ from standard network-layer attacks because they use valid service requests (e.g., HTTP GET/POST) to create overwhelming traffic for target nodes. The attacks resemble normal network traffic, which makes them extremely hard to detect with traditional intrusion detection systems focusing on packet structure and network behavior anomalies.

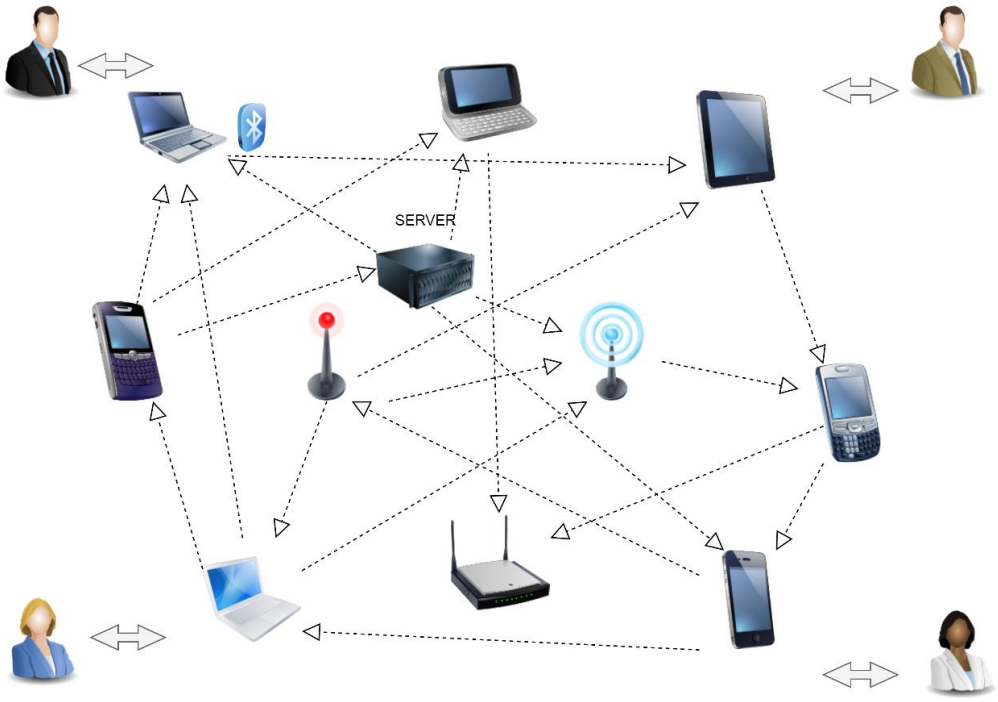


Figure 1: MANET

The security environment continues to expand because of multiple recent instances. Cloudflare achieved its highest DDoS protection record in June 2025 by stopping 7.3 Tbps traffic, which resulted in 37.4 TB of data transfer in under 45 seconds [29] [30] [31]. The attacks against traditional infrastructure demonstrate that smaller-scale attacks would be enough to disrupt resource-constrained MANETs. The Radware Cyber Threat Report 2025 showed HTTP-based application-layer attacks surged by 550% while Imperva recorded a 548% increase in telecom-sector application-layer DDoS attacks throughout the opening quarter of 2024. The majority of these threats came from compromised wireless and IoT endpoints, which demonstrated an alarming connection between wireless expansion and adversarial botnet growth [32] [33] [34].

Decentralized networks like MANETs are seriously at risk from DDoS attacks, which are becoming more sophisticated and widespread, according to recent reports. The viability of using mobile devices in DDoS campaigns was demonstrated in a well-known case where attackers took control of mobile ad networks to produce up to 4.5 billion HTTP requests daily [13]. The vulnerability of MANETs to flooding-based attacks, such as RREQ and Hello floods, which can interfere with routing and divide the network in the presence of dynamic node mobility, is further supported by scientific research [14]. As per technical analysis, MANETs are susceptible to resource depletion attacks due to elementary yet prevalent flood approaches owing to the decentralized nature of MANETs [15]. In addition, according to NETSCOUT cybersecurity professionals, botnets powered by AI are nowadays automating DDoS attacks, greatly escalating the magnitude and stealth of such botnets, posing an imminent threat to low-power and infrastructural-less networks such as those found in MANET environments [16].

The nodes that form MANETs are networked with the potential to act as devices that facilitate routing and host systems that make them susceptible to minimal security breach causes that can lead to significant network performance degradation due to routing failure and packet loss with increased latency and complete loss of service. The lack of centralized control and dynamic topology changes within MANET environments inhibit the effectiveness of traditional security measures due to MANET devices' lack of resources such as battery energy. The use of MANET DDoS applications becomes particularly destructive and potentially only within critical delay applications that require immediate action to save lives. The attackers are responsible for carrying out these activities to complete their objectives through the development of fraudulent traffic scenarios that simulate emergency communication spikes and flash crowds. The innocent traffic is potentially identified as malicious with resultant false positive instances with the aim to conceal real attack instances that result in false-negative instances. A traffic analysis system must be capable of evaluating data statistically and in contextual settings to identify subtle variations between normal and fraudulent network traffic. Static approaches to traffic analysis are potentially counterproductive as normal operating factors that potentially occur during crisis and peak use scenarios are potentially similar to factors that are potentially identified as suspicious with the potential to be labeled as normal use factors during critical and crisis use periods.

The process of attack detection calls for real-time mitigation and is the next crucial step. Static measures and resource-hungry processes are not practical approaches to take in MANET environments. The existing solutions are unable to change attack reactions dynamically and result in increased detection times and unintentional damage to normal network communication. A defensive solution should integrate the application of lightweight intelligent resources that ensure the operations involving the Quality of Service (QoS) are protected during attack scenarios. The process of attack detection by means of the reaction process that has slower reactions might result in the blocking of critical packets while offering extended options and rapid draining of node battery resources to unacceptable ranges. The study aims to counter these challenges with the application of machine learning (ML) techniques. CNNs and RNNs are deep learning techniques that efficiently classified traffic in current applications. The analysis of traffic data through temporal or hierarchical patterns by these models produces better classification results than traditional rule-based methods. The existing research investigates specific elements of DDoS detection and mitigation and flash-event differentiation, yet it does not provide an integrated solution framework. Most existing solutions do not account for mobile node computational constraints, which makes them unsuitable for practical use in real-world scenarios. Models with deep architectures that provide good accuracy are not sustainable because nodes need to run their decision-making modules.

A cohesive framework that integrates dynamic routing features with DDoS detection capabilities is absent from the current implementation. Without load balancing or smart rerouting, attack detection is pointless

since it leads to traffic bottlenecks that hinder full mitigation. Aggressive filtering may unintentionally worsen user experience, which is why QoS preservation is frequently disregarded. Traffic shaping is rarely used in conjunction with selective forwarding or flow redirection as part of detection models in MANETs with limited resources. By offering SHIELD as a comprehensive, lightweight modular approach created especially for MANETs, this study tackles the current issues. The SHIELD framework combines Xavier-initialized SoftPlus CNN (XSP-CNN) with high-accuracy attack detection capabilities and uses Extra Trees along with Brownian-motion enhanced Harris Hawks Optimizer (BM-HHO) for feature-optimized mitigation and implements information divergence-based classification through Pearson correlation for flash crowd vs attack differentiation and adaptive routing through Interpolation-based Crossover-Mutation Invasive Weed Optimization (I-CMIWO) and Double Shift Right Complement (DSRC) mitigation layer.

The system architects created this single architecture to deploy in real time while ensuring experimental reproducibility, so it protects networks without diminishing system performance. This research builds on existing works by uniting detection with mitigation and differentiation, and adaptive routing to build a functional, deployable framework. The ultimate objective involves stopping service interruptions while maintaining network performance, together with reducing erroneous detections and protecting battery life and processing capacity during unstable traffic conditions.

Research has confirmed the existence of HTTP flood attacks combined with routing disruption attacks, which have targeted wireless-linked 5G and MANET-style deployments. Network filters become ineffective when attackers use TLS-handshake connection impersonation alongside malformed JSON payload injection and legitimate protocol reset manipulation. Low and slow attacks are worse because they use intermittent requests that slowly drain resources while remaining under traditional traffic rate thresholds. Traditional detection methods fail to meet these circumstances because they operate with static or threshold-based techniques, thus requiring adaptive intelligence-based solutions. Service disruptions lasting even a short time become extremely dangerous for both rural communities and combat zones. During the COVID-19 pandemic educational MANET deployments in distant zones lost critical functions because of application-layer flood attacks, which stopped instruction delivery for weeks. Field networks operated by military forces lost their ability to track command chain activity during short-term DDoS attacks. The real-world situations demonstrate that secure lightweight protection systems must be specifically designed for decentralized wireless environments that operate dynamically.

The research aims to fill the existing divide with novel intelligent DDoS protection solutions that are lighter and more intelligent, utilizing recent findings. The SHIELD framework sets up an entire defensive setup to ensure safe operations within the wireless ad hoc environment. The modular architecture facilitates modifications to the constituents without affecting the entire setup as the detection mechanism and mitigation process in conjunction with the routing process retain complete defensive setup capabilities. The synopsis proceeds to include the Literature Review section that examines the current research on detection techniques and mitigation techniques as well as flash event differentiation techniques. The Results and Discussion section evaluates the framework's performance through metrics and comparisons. The Conclusion and Future Scope section summarizes the contributions and recommends potential future research directions. The document ends with Publications and References, which validate the presented methodology through credibility and replicability evidence.

2. Literature Review

The defense strategy for protecting networks against DDoS attacks includes four stages which are prevention, detection, differentiation and mitigation. The complete taxonomy of DDoS Attack Management appears in Figure 2 demonstrates the different stages of a DDoS attack timeline. Prevention stands as the first stage of defense but due to increased tactics and humongous botnet it is very senseless to rely only on it.

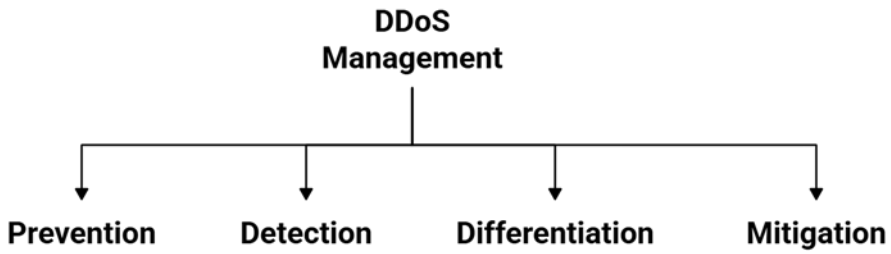


Figure 2: DDoS Attack Management

Research institutions now focus on application-layer DDoS attacks because they bypass numerous security measures operating below the application layer. The authors of Bhuyan et al. (2015) discuss DDoS attacks and defense mechanisms in detail and explain that application-layer attacks remain undetectable because they mimic typical network traffic [20]. Both signature-driven and anomaly-driven intrusion detection methods face difficulties when detecting these attacks because signature-based systems cannot identify new attack patterns, and anomaly detectors produce excessive false alarms when they mistake normal traffic spikes for malicious activities [17]. The 2016 Dyn attack presented a detection challenge to Woolf (2017) because attackers used normal DNS queries to fuel the flood. The lack of centralized monitoring across MANETs makes real-time detection even more challenging. The machine learning solutions for DDoS defense require ensemble models with feature selection that improves detection rates but increases system complexity [18].

The task of flash event detection during attack instances is still purely challenging. The study by Junhong (2021) made use of Pearson's correlation coefficient (PCC) to distinguish behavorial features that are distinct during flash crowds and attack instances [19]. The study managed to reduce false alarms by focusing on heavily correlated features that denote authentic traffic spikes but are only capable of pointing out linear features. The use of potential attack detection utilizing entropy estimation has been previously carried out by Timcenko et al. (2018) by pointing out traffic that denoted drastically low entropy values. The efficacy of such detection wanes during intense authentic traffic since various fresh connections can denote values that are drastically low and are unreflective of potential attack instances [22]. The use of machine learning classifiers to distinguish between flash crowds and attack instances was carried out by Ye et al. (2019), who managed to correctly distinguish attack instances with SVM classifiers. The efficacy of SVM classifiers and other similar models still faces various scaling challenges since such models are less accurate during instances that entail numerous features [23]. The process becomes greatly cumbersome

during MANET environments due to various large-scale data and features [23]. Deep learning models (CNNs & RNNs) denote paramount accuracy within the context of accurate DDoS traffic detection; however, such models are tasks that entail intensive computing processes (GPU & large-scale memories), which are uncharacteristic within MANET environments. Statistical features joined with Machine Learning models to distinguish instances with greater accuracy that denoted drastic decreases within false positives was previously carried out by research by Najafi Mehr et al. (2022), who denoted higher complexities within such processes [24]. The study demonstrates that various simplistic statistical processes entail lightweight processes; however, such processes denote unaccurate results since various evolved models such as Light-BGM & AO-ETC denote accurate results with higher consumptions [27] [28].

It has been proven in a number of research studies that load balancing and adaptive routing are basic aspects. The statistical DDoS countermeasure by Hajimatingshsoodi and Jalili (2022) is based on behavioral analysis and dynamic rerouting since these authors prove that rerouting is required to eliminate node bottlenecks [25]. Karpowicz (2021) investigated adaptive traffic policing to counter the DDoS attacks with the optimization of network parameters that contributed to avoiding congestion. This study has shown that it is important to allow networks to adjust their operational paths and transmission speeds in case of attack though the experiments were based on non-MANET networks. AODV and DSR routing protocols can be enabled with security layers to make node rerouting in MANETs possible. AODV system modified by Shalini et al. (2019) to include cooperative traffic dropping and legitimate traffic rerouting (DOCUS) also used pre-defined thresholds to operate, and no learning-based detection was used [21]. The findings provide an insight into one of the ways of incorporating intelligent detection functionality into routing control systems.

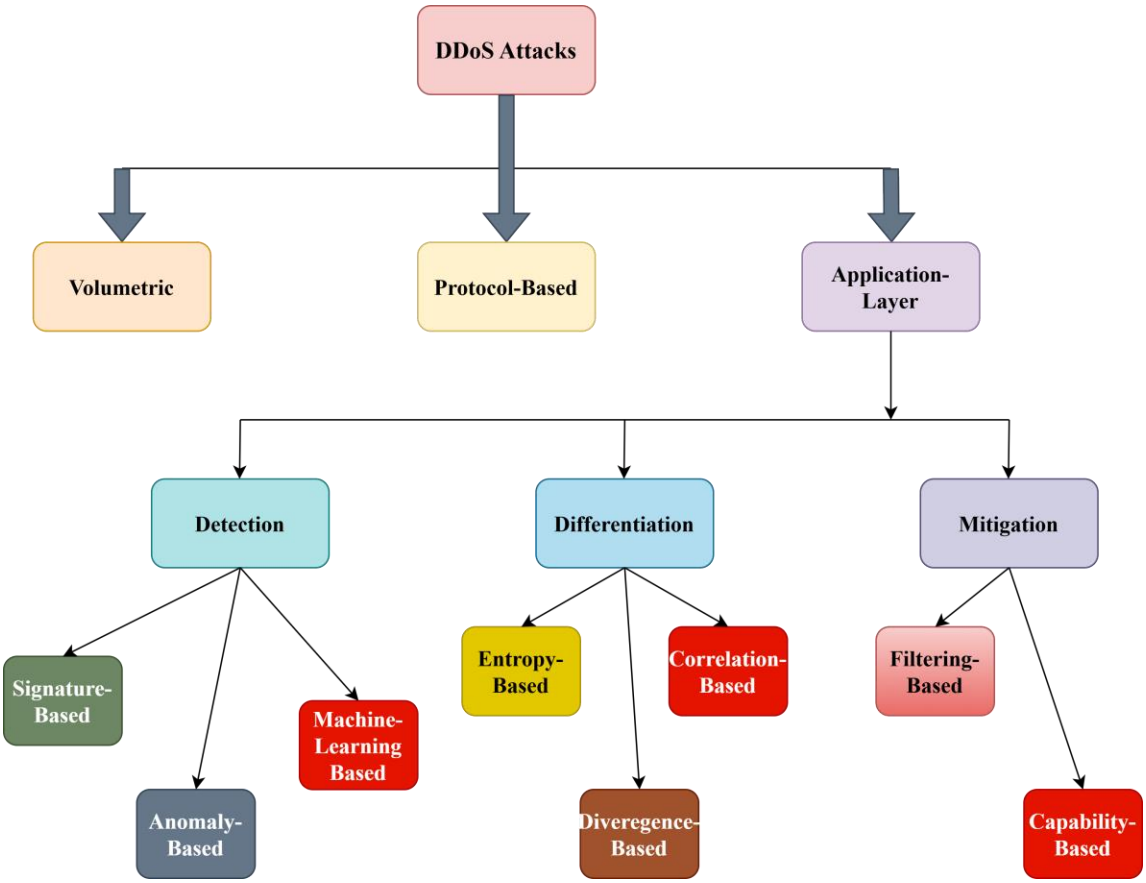


Figure 3: Taxonomy and Strategies for DDoS Attack Management

Figure 3 shows Taxonomy and Strategies for DDoS Attack Management and highlighted preferred method as solution. let's discuss the prominent works in each aspect and their constraints.

2.1 Detection of Application Layer DDoS Attacks

Saravanan et al. (2024) proposed an adaptive defense reinforcement methodology to secure IoT-enabled MANETs by continuously updating detection policies using fuzzy logic-based systems. The method demonstrated strong performance in changing environments yet failed to scale across different network topologies and did not differentiate between flash events and malicious traffic surges [1]. Vuyyuru et al. (2023) developed EsECC-SDN as a model for MANETs which uses entropy-based methods together with SDN architecture to classify DDoS attacks. The model depends on centralized SDN elements, which restricts its use in pure MANETs [2]. Kucukkara et al. (2024) generated a quantum-neural network-based platform-independent model for DDoS cataloguing. The research concentrated on cloud networks but provided minimal understanding about resource-limited MANET environments [3]. The majority of current models detect DDoS attacks in general terms without accounting for the distinctive decentralized structure and mobile node characteristics of MANETs. The identification of benign flash events continues to be insufficiently addressed.

2.2 Mitigation and Feature Optimization in MANET Intrusion Detection

The combination of metaheuristics and deep learning techniques offered by Albakri et al. (2023) offers superior malware detection results. The complexity of this method is so high that it is hard to apply it in MANETs since the efficiency of energy usage is crucial [4]. Simsek and Toklu (2018) invented dual-layer mitigation framework that used both rate-based control and the use of traffic filtering. The technique is effective against high rate DDoS attacks and generates excessive false positives with low rate applications layer attacks and adds high latency [5]. Invasive weed optimization was applied by Mohammed (2021) to detect cloud ransomware. A balanced speed-energy consumption trade-off was obtained by use of IWO routing load balancing implemented in the framework [6]. The existing mitigation methods need a considerable amount of computational power and do not involve the aspect of feature selection. The existing frameworks do not have light-weight solutions that are adaptable to the requirements of MANET environment, which support the limited energy resources and dynamic nature.

2.3 Flash Crowd Differentiation and Unified Framework Approaches

Guelfi et al. (2022) used divergence metrics to differentiate flash crowds in cloud environments, yet their method required testing under MANET-specific challenges such as frequent topology changes and dynamic routing [7]. Hekmati et al. (2023) developed Correlation-Aware Neural Networks (CANN) to identify DDoS traffic from legitimate usage spikes in IoT systems. The powerful framework requires hardware accelerators for real-time correlation computation but these accelerators might not exist in MANET nodes [8]. Gautam and Tokekar (2020) studied lightweight detection models for MANETs, yet failed to achieve modularity because they did not integrate detection with flash analysis and routing into a single system [9]. David et.al. proposed Threshold updater to distinguish flash crowd and DDoS attack [10]. Mihanjo et. al used deep learning method to achieve same refinement [11]. A complete framework which unites traffic analysis with optimized mitigation and flash event distinction, and routing functions does not exist for MANETs. Table 1 presents recent DDoS attack solutions with their main findings and areas for improvement for detection, mitigation and differentiation approaches.

Security models currently focus on one aspect of security, which includes detection or mitigation or differentiation. Flash events continue to cause false positives which result in the denial of legitimate service. Lightweight models with feature selection and modular integration for constrained MANETs are rarely used in current research.

Table 1: Investigation of Prevalent Algorithms against DDoS Attack

Year	Title	Authors	Approach	Significant Findings	Work Need to be Addressed
2024	"Enhancing IoT security in MANETs: A novel adaptive defense reinforcement approach"	S. Saravanan et al.	Adaptive fuzzy-based defense	Dynamic response, better attack detection	Not scalable for heterogeneous networks and flash events not covered.
2023	"EsECC_SDN: Attack detection and classification model for MANET"	V. A. Vuyyuru et al.	SDN-based entropy model	Noble grouping appearance in hybrid networks	Relies heavily on SDN for accurate results
2024	"Quantum-neural network model for DDoS classification"	M. Y. Kuçukkara et al.	Quantum-enhanced deep learning	Amazing detection precision	Non-resource aware for battery constrained devices
2023	"Metaheuristics with deep learning for malware detection"	A. Albakri et al.	Metaheuristics + CNN	Robust detection	High complexity
2018	"Two-layer approach for mixed-rate DDoS attack detection"	M. Simsek & M. Toklu	Traffic filtering and rate control	Effective against high-rate attacks	Not effective for application layer attacks, and suffer from delay problems
2021	"Invasive Weed Optimization for cloud ransomware detection"	A. H. Mohammed	IWO optimization technique	Upgraded attack isolation in the cloud	Not designed for mobility and real-time routing
2022	"Distinguishing DDoS Traffic in Flash Crowd Environments"	A. E. Guelfi et al.	Divergence metric analysis	Reasonable success in cloud flash situations	Not validated for diversity of topology and routing

2023	"Correlation-Aware Neural Networks for DDoS Detection"	A. Hekmati et al.	Pearson correlation + CANN	High accuracy flash vs. attack classification	Requires higher processing capacity
2013	"A Novel Solution to Handle DDoS Attack in MANET"	Chhabra et al.	AODV/DSR modifications via NS-2	Compact packet loss, enhanced throughput	mobility overhead unmeasured
2012	"Explicit Query Based Detection"	Singh et al.	Sequence-number analytics	Detected inconsistent request behavior	High false positive
2016	"DOS Attack Mitigation in MANET"	Garg & Sharma	IP broadcast control	Recognized flooding trend behaviors	No real deployment
2017	"Preventive Mechanism in MANET"	Ahamad & Aljumah	Threshold comparison	Initial detection of high ingesting nodes	no real network test
2021	"Entropy-based DDoS Attack Detection in Cluster-based MANETs"	Deepa Dhindsa & K. S. Dhindsa.	Shannon Entropy, Packet Rate Analysis	Distinguished 95% of attacks with a low false alarm rate	Not a scalable under a dynamic topology
2025	"Lightweight ML framework for efficient DDoS detection in IoT"	Nawaz, M. et al.	SVM, DT, KNN, RF	Attained 99.1% detection with a lightweight model	Unverified in Real time IoT Scenarios
2024	"Proactive DDoS detection via marking, analysis and ML"	Pasupathi, R. et al.	KNN, RF, SVM, XGBoost	KNN attained 98.4% accuracy with good traceability	Scalability and latency under real-time load not evaluated.
2024	"Leveraging blockchain & ML to counter DDoS in IoT"	Kumari, R. et al.	ANN, KNN, Random Forest	High 99.3 % accuracy with secure decentralized authentication	Increased delay of block chain consensus processing

Modern attackers use IP address rotation, browser fingerprint duplication and expensive endpoint exploitation to bypass preventive security measures which either restrict legitimate users or fail to stop evolving traffic attacks which make prevention schemes absolute. For detection of application layer DDoS Attack the machine learning based methods catches what signatures based method miss such as bots that mimic real users, rotate payloads, or hide behind TLS. It learns normal behavior-request mix, timing, paths-

and flags patterns that don't fit, even when attackers change tactics. Capability-based mitigation protects the web-app without harming real users. Instead of blunt rate limits, clients earn service-tokens, proofs, session trust, or reputation-and keep it during stress, while bots get throttled or dropped. Correlation based methods separates an attack from a genuine surge by tying signals together across users and time: synchronized think-times, common fingerprints, same AS clusters, or identical navigation paths. That's where simple entropy or divergence checks usually stumble-they light up on any busy day. This makes MANET systems to adopt real-time detection and mitigation capabilities to analyze user actions for intent identification, abuse detection, automatic load management through traffic redirection, content caching and service degradation.

2.4 Identified Research Gaps

By virtue of the exploration of prevalent techniques, the following Research Gaps were identified.

- **Real-Time DDoS Detection:** For detection of application layer DDoS Attack, the proposed method should catch bots that mimic real users, rotate payloads, or hide behind TLS. It should learn normal behavior-request mix, timing, paths-and flags patterns that don't fit, even when attackers change tactics.
- **Reliable Flash Crowd Discrimination:** The current methods incorrectly identify regular flash crowds as DDoS attacks. A stronger divergence-based analysis needs to be developed to eliminate these incorrect positive results.
- **Adaptive Routing in Mitigation:** The current DDoS mitigation strategies fail to implement on-the-fly routing adjustments together with distributed load balancing. Network congestion and single points of failure will occur in networks that do not implement this solution even after attack detection.
- **MANET-Specific Adaptability:** Many models which are not designed for MANET's dynamic resource-constrained environment have limited scalability and resource awareness. Solutions must be lightweight and adaptive.
- **QoS Preservation:** The defense strategies that focus on stopping attacks usually disregard the QoS requirements for legitimate users during the mitigation process. The problem of maintaining minimal service degradation is not addressed in most cases.
- **Unified Defense Framework**: Most research works focus on solving specific parts of the problem (detection only, or mitigation only, etc.) in separate silos. A complete framework which integrates detection with mitigation and differentiation and routing functions does not exist.

Our research uses prior work insights to develop a complete solution which addresses these identified gaps. The following section describes our research objectives, which explains how these limitations can be addressed.

3. Objectives

Mobile-Ad-Hoc Networks serve critical functions through their deployment in military communications and disaster relief operations and vehicular networks, and remote monitoring systems. The open nature of their medium combined with their dynamic topology and decentralized control structure, makes MANETs highly susceptible to sophisticated security threats particularly application-layer Distributed Denial-of-Service (DDoS) attacks. The attacks use legitimate requests to create service overload, which traditional network-layer defenses cannot detect or mitigate effectively in MANET environments. The research implements SHIELD (Secure Hybrid Integrated Framework for Enhanced Defense and Load-balanced DDoS Mitigation) as a unified, lightweight framework to achieve the following structured objectives for effective threat mitigation.

3.1 Optimized Detection of Application Layer DDoS Attacks Using Traffic Analysis

The initial goal focuses on creating a real-time application-layer DDoS attack detection algorithm through traffic behavior analysis. A lightweight hybrid detection model should be developed for resource-constrained MANET environments to detect application-layer floods which resemble legitimate traffic patterns. The detection system utilizes XSP-CNN (Xavier-initialized SoftPlus CNN) as its custom Convolutional Neural Network variant to achieve smooth training convergence and stable gradient flow through SoftPlus activation.

3.2 Optimized Mitigation Using Feature Selection

The detection of an attack requires immediate and efficient mitigation procedures. The second objective presents a resource-aware mitigation approach designed for MANETs which must operate under limited battery power and processing capabilities. The BM-HHO (Brownian Motion-enhanced Harris Hawks Optimization) algorithm serves as the main component of this objective because it uses a nature-inspired metaheuristic to select the most relevant features which indicate DDoS behavior.

3.3 Accurate Differentiation of DDoS from Flash Events Using Information Divergence

MANETs face a significant challenge because it becomes difficult to differentiate between malicious traffic surges and legitimate high-load events that occur during emergency broadcasts. Service disruptions become harmful when flash crowds are mistakenly identified as DDoS attacks. The proposed solution tackles this issue by creating an advanced statistical system for differentiation. The system uses Pearson Correlation Coefficient (PCC) to evaluate the behavioral match between incoming traffic and established flash crowd profiles.

3.4 SHIELD: A Unified Framework with Optimized Routing and Resilient Defense

SHIELD represents the ultimate goal, which unifies detection capabilities with mitigation functions and differentiation methods into a unified powerful defense framework. SHIELD provides complete end-to-end protection for MANETs through adaptive traffic rerouting that maintains QoS while neutralizing threats.

The SHIELD system comprises four modules:

- Detection Engine: XSP-CNN (Xavier-initialized SoftPlus CNN)
- Mitigation Controller: BM-HHO (Brownian Motion-enhanced Harris Hawks Optimization)
- Differentiation Module: PCC (Pearson Correlation Coefficient) based classifier

• Routing Optimizer: A novel Interpolation Based Crossover Mutation Invasive Weed Optimization (I-CMIWO) algorithm along with a lightweight Double Shift Right Complement (DSRC) filtering mechanism. The following section describes our research methodology for each objective, which explains how the proposed research develop improved algorithms based on these limitations.

The Proposed research need a systematic model evaluation system which will use simulation testing and hardware testing as its two evaluation approaches. The evaluation method of simulation-based testing depends on controlled datasets which allow this research to perform multiple large-scale experiments. The research uses three essential sources from this category which include synthetic datasets that simulate particular attack and defense situations and the CIC DDoS 2019 dataset for studying distributed denial-of-service attacks and the EDGE IIoT dataset for representing contemporary industrial IoT systems under attack. The collected datasets enable proposed reseach to analyze system performance across various scales while evaluating precision levels and system stability under various operational scenarios. The evaluation process becomes more similar to actual deployment through hardware experiments. The process needs LOIC (Low Orbit Ion Cannon) tools to perform simulation attacks for testing defense systems through physical device deployment. The two methods operate together to create a system which combines controlled laboratory tests with actual field measurements.

4. Contributions

To achieve the research objectives, the proposed research designed a multi-module framework wherein each module addresses a specific aspect of the DDoS defense challenge. The methodology is empirical (based on observed network traffic patterns), methodical (each step is logically derived from the previous), and cyclical (with iterative refinement and validation at each stage). We emphasize reproducibility by clearly defining algorithms and using standard datasets. A high-level schematic of the proposed approach is presented in Figure 1**,** illustrating how detection, mitigation, differentiation, and routing modules interact in the SHIELD framework.

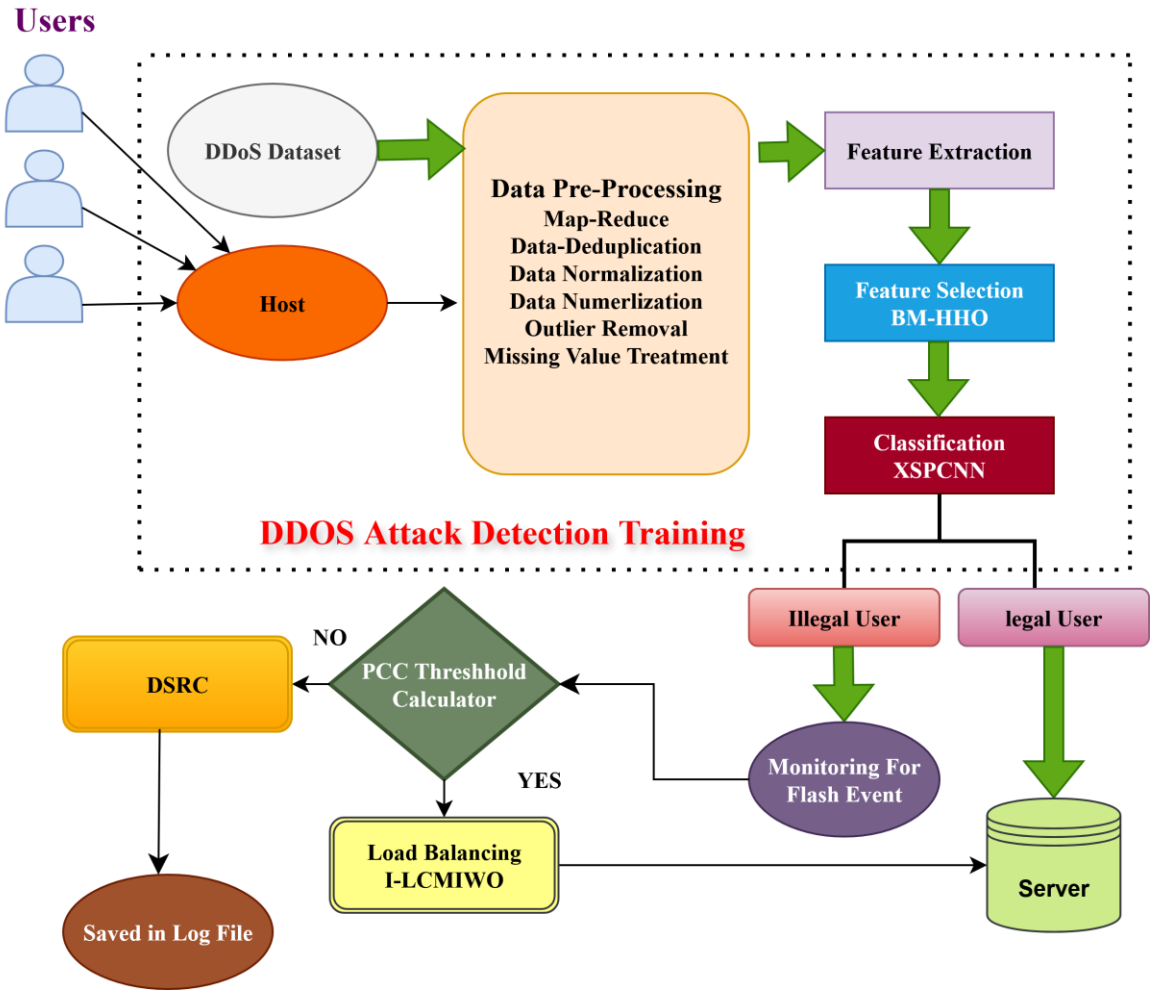


Figure 4: Block diagram of the proposed model

The MANET DDoS defense system uses the Integrated SHIELD framework architecture as portrayed in Figure 4. The system trains on a DDoS traffic dataset to develop an intelligent detection model (XSP-CNN classifier) with optimized features (via BM-HHO). The system classifies incoming traffic into legitimate and attack categories before directing legitimate traffic to Load Balancing (I-CMIWO) for optimal routing

and triggering DSRC mitigation for detected attack traffic. The PCC Threshold Calculator tracks network traffic behavior to identify flash events from actual attacks, so legal user surges are not mistaken for attacks. The complete loop protects servers and networks through efficient routing of benign traffic and real-time mitigation of malicious traffic.

4.1 Optimized Detection of Application Layer DDoS Attacks in MANET Using Traffic Analysis

Application-layer Distributed Denial of Service (DDoS) attacks have developed into one of the most complex threats against Mobile Ad Hoc Networks (MANETs) because they can imitate regular user activities. Standard requests such as HTTP GET and POST serve application-layer attacks to create server or application logic overload which does not produce traditional DDoS signatures at lower OSI layers. The attacks remain undetectable because they use authentic protocols and services to blend with typical traffic behaviors. MANETs face disastrous service interruptions and prolonged delays and increased energy consumption because of their limited resources while attacks remain hidden in normal traffic patterns. The research develops an optimized lightweight real-time application-layer DDoS detection system which addresses the unique requirements of MANETs. The main research objective involves developing an intelligent deep learning-based detection engine that analyzes traffic spatio-temporal patterns without placing excessive demands on network nodes. The implementation of this hypothesis requires three fundamental considerations:

- A detection algorithm needs to recognize and learn sophisticated traffic behaviors that develop throughout time.
- The model architecture must be designed for low computational requirements and memory usage to support limited MANET node resources.
- A successful feature extraction and training approach requires using standard traffic attributes alongside MANET-specific attributes to improve detection accuracy.

The XSP-CNN presents an innovative solution to real-time traffic classification that achieves both high detection accuracy and low computational resource usage. The primary purpose of creating the XSP-CNN is to address the weaknesses of existing detection models specifically their tendency to overfit and gradient vanishing problems and their scalability issues in MANET environments. RNNs and LSTM networks and Deep Belief Networks (DBNs) demonstrate success in static server-based environments but lack optimization for real-time operation in resource-limited applications. The models tend to be resource-intensive while requiring long training periods and extensive data sets. These detection models struggle to function effectively in the variable network configurations and sporadic connectivity of MANETs.

The proposed detection model includes multiple strategic design choices to enhance performance together with robustness and deployability. The Xavier initialization method produces stable gradient flows which leads to faster and more dependable training convergence. The SoftPlus activation function provides a smooth output for negative inputs which helps prevent dead neurons and allows continuous learning by contrast to ReLU. The 1D convolutional architecture effectively extracts temporal characteristics in network traffic data through inter-arrival times and session patterns which makes it an effective tool for identifying application-layer DDoS attacks. The model implements resource-aware design principles with decreased parameters and batch normalization and 16-bit weight quantization which enables it to run on Raspberry Pi or Android-based MANET nodes without performance degradation.

4.1.1 Dataset Preparation

The creation of realistic MANET behavior and conventional attack datasets required generating synthetic data through the combination of CIC-Darknet2020 with NS-3 simulations of MANET-specific mobility and routing characteristics. The CIC-Darknet2020 dataset contains extensive malicious and benign traffic patterns yet it does not replicate the decentralized mobile network characteristics of MANETs. We developed NS-3 simulation models using Random Waypoint and Gauss-Markov to simulate node mobility and dynamic topology for bridging the gap between CIC-Darknet2020 and MANET characteristics. The simulations recorded hop count data along with node mobility speed and link stability and TTL variations for all node pairs during packet transmission. The logged parameters received shared identifiers such as timestamps and flow metadata (e.g., source-destination IPs) to merge with CIC-Darknet2020 flows through programming. The hybrid dataset maintains CIC-Darknet2020 attack signatures while incorporating realistic MANET constraints through multi-hop routing and node movement. The model training becomes more relevant through this augmentation because it learns to perform better in the dynamic resource-constrained environments which are typical for MANET deployments. The classifier training step needs a DDoS dataset to train the model for identifying user requests as either legitimate or non-legitimate. The training process includes pre-processing followed by feature extraction and feature selection and classification. The DDoS dataset underwent pre-processing before being ready for the training classifier. The DDOS dataset provides the following input data,

$$T_{(d)} = \left[T_{d1}, T_{d2,}, T_{d3,\ldots,}, T_{da}\right] \quad (1)$$

Here, T_{da} denotes the a^{th} input data sample.

First, an important step to follow while training the data is Data Pre-processing to improve classification accuracy. The pre-processing phase involved removing duplicate records and standardizing the data to determine whether they were numeric or non-numeric. The first step for improving classification accuracy involves pre-processing which enables us to focus on deduplication and normalization. The MapReduce framework enables the removal of duplicate entries through de-duplication processes. The map duty divides input data into key-value sets before the reduction process merges different keys with their values into one unique record that eliminates duplicates. The cleaned multi-matched data is now prepared for analysis and training purposes. From the Map Reduce technique, the obtained non-duplicate data $T_{d(nd)}$ is finally expressed as,

$$T_{d(nd)} = [T_{d(nd1)}, T_{d(nd2)}, T_{d(nd3)}, \ldots, T_{d(ndJ)}] \quad (2)$$

Here, $T_{d(dnJ)}$ denotes the J^{th} non-duplicate data instance.

Even after deduplication, the dataset contains non-numerical data such as strings and Boolean valuesFor subsequent classification, all non-numerical attributes were converted into numerical form. In this step, categorical or textual fields are mapped to corresponding numeric representations. The resulting numeric dataset is denoted as $\left(T_{d(num)}\right)$ and is obtained as:

$$T_{d(num)} = [T_{d(num1)}, T_{d(num2)}, \ldots, T_{d(numb)}] \quad (3)$$

Here the b^{th} numeralized data is implied as $T_{d(numb)}$.

Data normalization is performed to gauge the values in an exact assortment which helps accelerate the training process. For this purpose, Z-score normalization is used, which standardizes the numeric data by scaling each value so that the dataset will have a mean of 0 or Standard Deviation (SD) of 1. Normalizing

such a means that the data have a zero mean and a variance equal to 1, that is, they are scaled down to obtain a normal distribution of values for each feature. Z-Score normalization is utilized to normalize the numeralized data ($T_{d(num)}$). The process of normalising every value in the data such that the average of all values is 0, and the Standard Deviation (SD) is 1. The normalized data ($T_{d(norm)}$) is provided by,

$$T_{d(norm)} = \frac{(T_{d(\text{num})} - \overline{T_{d(\text{num})}})}{\alpha_{(T_{d(\text{num})})}} \quad (4)$$

Here, $\overline{T_{d(\text{num})}}$ denotes the mean of the numerically transformed data, while $\alpha_{(T_{d(\text{num})})}$ represents its standard deviation.

4.2 Optimized Mitigation Using Feature Selection in Resource-Limited MANET Nodes

After implementing accurate malicious application-layer traffic identification through optimized detection methods in Objective 4.1, the following priority involves quick and efficient attack mitigation that preserves legitimate communication. Mobile Ad Hoc Networks (MANETs) face unique challenges in mitigation efforts because their fundamental limitations include restricted battery life and dynamic topologies and processing constraints and decentralized network structure.

Any elementary mitigation strategy that achieves packet dropping or blacklisting in the detection results alone can find itself damaging the legitimate users in the false positive cases. Such failure of the rule-based defensive systems to respond dynamically prevents them to be effective against new or malicious patterns of DDoS attacks. This study suggests a smart multi-layered mitigation system, which incorporates optimization of features with adaptive response mechanisms to provide accurate protection at a minimum cost and minimal disruption to normal operations.

The mitigation strategy will be reliant on Feature Selection Optimization as its primary basis to remove superfluous traffic attributes and focus defense resources on the most significant features. The Brownian-motion Harris Hawks Optimization (BM-HHO) algorithm has more sophisticated features to carry out this strategy. The BM-HHO algorithm is capable of making the feature space of mitigation logic efficient as well as highly discriminative that allows fast and accurate interventions. Conventional mitigation solutions give an equal priority to all traffic characteristics but have strict limits that produce a vulnerability to threats and cannot work in noisy scenarios. DDoS attacks that occur at the application-level pose certain challenges that influence their alleviation.

The attackers construct attack traffic in such a way that it will not be discovered by out-of-date signature. The flash events that possess high legitimate traffic volumes can lead to undesirable rate-limiting due to their nature. The features of monitoring that are not important result in undue mitigation costs that are greater than the real threat. There are additional challenges associated with MANETs due to their nature which include: The nodes within the network do not possess sufficient processing power to enable them to provide high-dimensional analysis in real-time. Over use of sophisticated filters leads to loss of battery due to high usage of the CPU. The mitigation rules must be able to change as quickly as the patterns of routes and the dynamics of the network flow. The considered choice of optimized features minimizes computation costs and ensures higher speed as well as more accurate response. The system allows the adjustable response mechanisms in accordance with the identified types and the level of severity of anomalies.

4.2.1 Implementation of BM-HHO as meta-heuristic optimization method

The Brownian-Motion Harris Hawks Optimization (BM-HHO) algorithm serves to improve this selection by identifying the optimal feature subset which offers the highest accuracy with minimal overhead.

BM-HHO Workflow:

1. Population Initialization:

Each hawk in the population serves as a potential feature subset through binary vector representation. Each hawk receives fitness evaluation through F1-score measurements from Extra Trees or LightGBM classifiers that operate on selected features.

2. Exploration Phase:

Hawks use Brownian motion perturbations for global searches to discover new areas and break through local optimal solutions.

The probability for a hawk to switch from exploration to exploitation depends on the escape energy of the prey which uses a dynamic convergence threshold based on fitness variance.

3. Exploitation Phase:

The best-performing solution attracts hawks through position updates that mimic both surprise pounces and cooperative hunting behavior.

The system performs logical crossover operations to breed feature subsets which demonstrate high scores in overlapping areas.

4. Termination:

The final mitigation feature set selection occurs when either 100 iterations pass or the fitness improvement remains below 0.01 for ten consecutive iterations. Algorithm 1 illustrates proposed BM-HHO.

From the cleaned dataset, we then isolate the most relevant attributes, including source IP address, timestamp records, source and destination ports, flow duration, destination IP address, total backward packets, total forward packets, and the communication protocol. The resulting feature set is denoted as (P_{ext}) and can be represented as,

$$P_{ext} = \left\lfloor P_{ext}(1), P_{ext(2)}, \dots, P_{ext(c)} \right\rfloor \tag{5}$$

Here the c^{th} number of extracted features is proposed by $P_{ext(c)}$.

The fitness value was computed for all possible solutions in each iteration. The fitness value is computed based on the classification accuracy. Two diverse strategies were utilized by the Hawks that are expressed mathematically as,

$$P(s+1) = \begin{cases} P_{rad}(s) - \beta_1 |P_{rad}(s) - 2\beta_2 P(s)| & , e \geq 0.5 \\ \left(P_{prey}(s) - P_n(s)\right) - \beta_3 \left(l_b + \beta_4 (u_b - l_b)\right) & , e < 0.5 \end{cases} \tag{6}$$

Algorithm 1: Brownian motion-based Harris Hawks Optimization (BM-HHO)

Input: Set of extracted features (F_{ext})

Output: Subset of optimum selected features $(F_{(selet)})$

Begin

Initialize population (F_{ext}), number of iteration $(s_{\max})$

Evaluate fitness value

Set the location of the prey as best location

While $(s \le s_{\max})$

Update E_{prey} using equation (8)

If $(E_{prey} \ge |1|)$

\\ Exploration stage

Update position of hawks using (6)

Else $(E_{prey} < |1|)$

\\ Exploitation stage

If $(\varepsilon \ge 0.5 \; and \; |E_{prey}| \ge 0.5)$

Update position of hawks using (9)

Else if $(\varepsilon \ge 0.5 \; and \; |E_{prey}| < 0.5)$

Update position of hawks using (12)

Else if $(\varepsilon < 0.5 \; and \; |E_{prey}| \ge 0.5)$

Update position of hawks using (17)

Else if $(\varepsilon < 0.5 \; and \; |E_{prey}| < 0.5)$

Update position of hawks using (17)

End If

End If

End While

Return optimal selected features

End

In this formulation, s denotes the current iteration index. The hawk's position at the next iteration is represented by $P(s+1)$, while $P_{rad}(s)$ indicates the position of a randomly selected hawk in the population. The present position of the hawks at iteration s is written as $P(s)$ and the prey's location is given by $P_{prey}(s)$. The parameters $P_{prey}(s)$, $\beta_1, \beta_2, \beta_3, \beta_4$ and e are random variables drawn from the interval (0,1). The symbols l_b and u_b denote the lower and upper bounds of the search variables, respectively. Furthermore, $P_n(s)$represents the mean position of all hawks at iteration s, and it is computed as:

$$P_n(s) = \frac{1}{c}\sum_{k=1}^{c} P_k(s) \qquad (7)$$

Where the position of each hawk is notated as $P_k(s)$.

The main statistic in the evolution phase is the escape of prey, which is mathematically articulated as,

$$E_{prey} = 2\hat{E}_{prey}\left(1 - \frac{s}{s_{\max}}\right) \quad (8)$$

The initial energy of the prey, which varies randomly within the range (−1,1), is denoted by $\hat{E}_{prey}$ while s_{max} represents the maximum number of iterations. The hawks remain in the exploration phase as long as the absolute energy satisfies $E_{prey} \geq |1|$. When the energy drops below this threshold, i.e., $E_{prey} < |1|$, the algorithm shifts to the exploitation phase and the prey's position is progressively refined.

The hawk confronted the prey by exploiting the four hurtling policies and prey-escaping conduct during the exploitation step. For an effective attack, escape energy and escape are obligatory. When, is the potential of escaping pretentiously that the prey has escaped efficiently? The prey does not efficaciously escape when $E_{Prey} \geq 0.5$

When $\epsilon \geq 0.5$. and $|E_{prey}| \geq 0.5$, the prey still possesses relatively high energy but exhibits a limited tendency to escape. Under these conditions, the hawks employ the soft besiege mechanism to gradually encircle the prey. This behaviour can be expressed mathematically as:

$$P(s+1) = \Delta P(s) - E_{\text{prey}}\left|b_m(m)P_{\text{prey}}(s) - P(s)\right| \quad (9)$$

$$\Delta P(s) = P_{\text{prey}}(s) - P(s) \quad (10)$$

Where the variation between the prey's and hawks' current position is modelled as $\Delta P(s)$, the prey random jump procedure is indicated as $b_m(m)$, which is computed utilizing the Brownian motion technique.

$$b_m(m) = \tau(\nu(m))^{\kappa} \quad (11)$$

Where the constant is signified as τ, the number of sudden motions is notated as ν, the diffusion parameter is symbolized as κ, and the prey random jump procedure is indicated as m.

When $\epsilon \geq 0.5$ and $|E_{prey}| < 0.5$, both the prey's energy and its ability to escape are significantly reduced. In this scenario, the hawks switch to a hard besiege strategy, fully surrounding and aggressively constraining the prey. This behaviour is modelled mathematically as:

$$P(s+1) = P_{\text{prey}}(s) - E_{\text{prey}}|\Delta P(s)| \quad (12)$$

When $\epsilon < 0.5$ and $|E_{prey}| \geq 0.5$, both the prey's energy and its tendency to escape are relatively high. Under these conditions, the hawks adopt a soft besiege with progressive rapid dives, during which they approach the prey through smooth, gradually intensifying dives. In this phase, the hawks update their positions in two steps. First, they estimate the prey's likely future movement and start moving towards it accordingly, which can be written as:

$$U = P_{\text{prey}}(s) - E_{\text{prey}}\left|mP_{\text{prey}}(s) - P(s)\right| \quad (13)$$

Where J = jump strength modelled using Brownian motion, Pprey = position of prey & E= escape energy

Thus, the location of the restructured hawk is assessed by exploiting equation (9), and the optimum features were selected by the proposed model employing BM-HHO as of the mined features for supplementary sorting in a similar way to aggressive prey based on convincing approaches.

In the second step, the hawks determine whether a dive should be executed. If a dive is selected, their irregular plunging behavior is modeled using the Levy Flight (LF) pattern, which generates uneven, stochastic dive trajectories. This process is mathematically described as:

$$M = U + V \times \gamma(d) \tag{14}$$

In this context, d denotes the dimensionality (size) of the optimization problem, V represents a randomly generated vector, and γ refers to the Levy Flight (LF) step, which is calculated using:

$$\gamma = 0.01 \times \frac{g \times \eta}{|h|^{\frac{1}{\lambda}}} \tag{15}$$

$$\eta = \left(\frac{\mu\left(1+\lambda*\sin\left(\frac{\pi\lambda}{2}\right)\right)}{\mu\left(\frac{1+\lambda}{2}\right)*\lambda*2^{\left(\frac{\lambda-1}{2}\right)}} \right)^{\frac{1}{\lambda}} \tag{16}$$

Here, η denotes random values drawn from the interval (0,1), λ is a constant parameter fixed at 1.5, and μ represents the standard gamma function. The fitness of each solution is evaluated based on the corresponding classifier accuracy. Accordingly, the updated position of the hawks can be defined as:

$$P(s+1) = \begin{cases} U & , \text{if it}(U) < fit(P(s)) \\ M & , \text{if it}(M) < fit(P(s)) \end{cases} \tag{17}$$

When $\epsilon < 0.5$ and $|E_{prey}| < 0.5$, the prey still attempts to escape despite its relatively low energy. Under these circumstances, the hawks employ a hard besiege with progressive rapid dives, combining tight encirclement with aggressive plunging maneuvers. In this phase, the vectors U and M are computed as:

$$U = P_{\text{prey}}(s) - E_{\text{prey}}\left|mP_{\text{prey}}(s) - P_n(s)\right| \tag{18}$$

$$M = U + V \times \gamma(d) \tag{19}$$

Thus, the updated hawk's position is evaluated by utilizing the equation (16).

After the feature selection, the optimal features were used to train the X-SPCNN classifier. This is an enhanced CNN using the Xavier initialization method and Soft Plus activation function. Figure 5 illustrates architecture of X-SPCNN classifier.

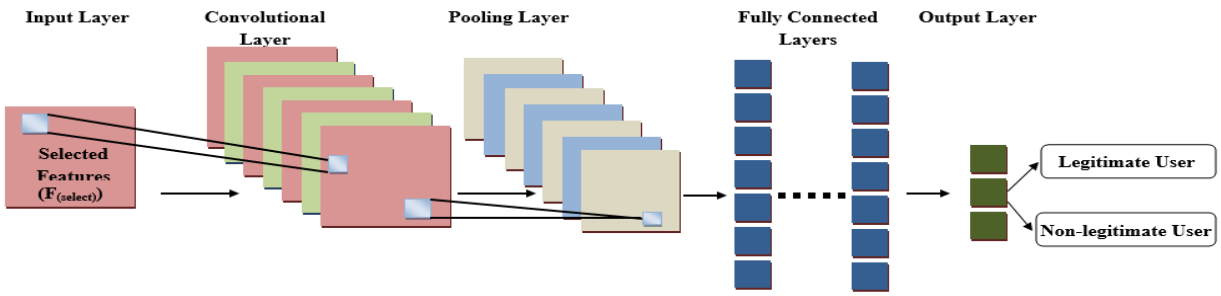


Figure 5: Architecture of X-SPCNN

The CL's output (Con_{lyr}) is expressed as,

$$Con_{lyr} = \mu\left(\sum_{i_n} \sum_{p,q} \mathrm{F}_{(\mathrm{selet})}{}^{w}\right) \quad (20)$$

Where the channel index is indicated as i_n, the coordinates of optimal features ($F_{(selet)}$) are notated by (p, q), the convolutional kernel is provided by w, which are randomly taken and the Softplus Activation function is signified as μ which is a ReLU function's smooth approximation utilized to constrain the output to be always positive. The Softplus Activation function can be articulated as,

$$\mu = \ln\left(1 + e^{F_{(\mathrm{selet})}}\right) \quad (21)$$

After each convolutional layer (CL), a pooling layer (PL) is applied to shrink the spatial dimensions of the feature maps and thereby reduce the computational burden. The PL operates on small local patches of the convolution output and replaces each patch with a single representative value through sub-sampling. The resulting pooled feature map, denoted as ($pool_{lyr}$), is obtained as:

$$\mathrm{pool}_{lyr} = down\left(\max\left(Con_{lyr}\right)\right) \quad (22)$$

In this context, the down-sampling operation that preserves the maximum value within each pooled region is denoted as $down(max(Con_{lyr}))$. Once all convolution and pooling operations are completed, the resulting feature maps are flattened into a single one-dimensional vector (f). This flattened vector serves as the input to the fully connected layer (FCL). The FCL behaves as a standard feedforward neural network: it multiplies the input vector by a weight matrix (W) and adds a bias vector (B_{ias}) at each neuron. To ensure stable activation magnitudes and improve training convergence, the weights in this layer are initialized using the Xavier initialization strategy. Accordingly, the initial weights are computed as:

$$W = \pm \frac{\sqrt{6}}{\sqrt{f_r + f_{r+1}}} \quad (23)$$

Here, f_r denotes the number of input connections to a neuron in layer r, while f_{r+1} represents the number of output connections from that neuron to the subsequent layer. Based on these definitions, the output of the fully connected layer, (ful_{lyr}), is computed as:

$$ful_{lyr} = \rho(\sum Wf + B_{ias}) \quad (24)$$

The final class probabilities are produced using the SoftMax activation function ρ, which is defined as,

$$\rho = \frac{\exp(f)}{\sum \exp(f)} \quad (25)$$

After this stage, incoming requests are examined for potential flash events prior to initiating any mitigation actions on traffic originating from legitimate users.

4.3 Differentiation of Application-Layer DDoS Attacks from Flash Events in MANET Using Information Divergence

The distinction between Application Layer DDoS attacks and flash events in Mobile Ad Hoc Networks (MANETs) requires sophisticated analysis. The two phenomena produce identical traffic surges which share comparable volume characteristics and behavioral patterns during initial observation. The fundamental difference exists between their intended purposes and resulting effects. Flash events occur naturally from user activity because of real-world triggers such as viral content or emergency broadcasts, whereas DDoS attacks represent malicious coordinated efforts to flood network services.

The current detection systems tend to mix up these two types of events because they share common characteristics including high request rates and burst traffic patterns and simultaneous access to similar resources. The consequences of incorrect classification remain severe. The incorrect identification of flash events as attacks leads to improper service denial for genuine users. The misidentification of DDoS attacks as flash crowds makes the system exposed to ongoing service disruptions. This objective aims to create an effective Differentiation mechanism because traditional MANET security systems lack this capability or have it poorly developed.

4.3.1 Methodology Overview

High-fidelity differentiation requires a multi-layered system which uses information divergence and Pearson Correlation Coefficient (PCC) analysis and machine learning classifiers trained on different traffic features. The fundamental principle states that flash events maintain statistical features of normal traffic because they show diverse access patterns and temporal entropy and heterogeneous user profiles despite their heavy volume. DDoS traffic differs from legitimate traffic because it demonstrates uniformity while being artificial and showing irregular timing patterns and repetitive behavior.

The first step involves statistical correlation models that identify temporal and structural similarities between present traffic surges and recorded flash event profiles. The system performs entropy-based divergence calculations after which it trains a binary classification model to identify traffic surges through enhanced features. The combination of these techniques establishes a multi-check pipeline which protects against both false positive and false negative traffic classification errors.

4.3.2 Pearson Correlation-Based Similarity Analysis

The Pearson Correlation Coefficient (PCC) is leveraged as a first-tier similarity test. PCC quantifies the linear correlation between two datasets, in our case, between an ongoing traffic burst and a reference flash event profile. When the system receives a very large volume of legitimate requests (lR). it uses the Pearson Correlation Coefficient Threshold (PCC) to detect possible flash events. PCC quantifies both the strength and direction of the linear relationship between the previous legitimate request sequence (lR_{pr}) and the current legitimate request sequence (lR_{cr}), and is calculated as:

$$T_{pc} = \frac{\sum\left((R_{pr}-\overline{lR_{pr}})(lR_{cr}-\overline{lR_{cr}})\right.}{\sqrt{\sum\left(lR_{pr}-\overline{lR_{pr}}\right)^2\left(R_{cr}-\overline{lR_{cr}}\right)^2}} \quad (26)$$

Where the preceding application's mean values are notated by $\overline{lR_{pr}}$, the mean values of the current request are signified by $\overline{lR_{cr}}$, along with PCC is proffered by (T_{pc}). The entire legitimate request will be subjected directly to mitigation if the authentic demand is under the threshold (T_{pc}). Then, it is progressed to the load balancing segment.

we integrated K-means clustering and Pearson Correlation Coefficient (PCC) to improve the current detection of flash events. The proposed approach first clusters the similar genuine requests into different clusters and then examine the correlation within each cluster. To achieve this, the localized analysis through PCC is used to detect abnormal behaviour which could be a flash event while at the same time minimizing the number of false alarms.

As the third stage, a dedicated binary classification model is trained to distinguish flash events from DDoS attacks. The dataset used includes:

- Historical flash events from public datasets and controlled simulations
- Synthetic and real DDoS traffic samples (e.g., HTTP floods, Slowloris)

To maintain real-time performance, this classifier operates on the output from prior stages—triggered only when PCC scores are ambiguous (e.g., between 0.6 and 0.8), reducing computational overhead.

The Real-Time Flash-Attack Differentiation Workflow is designed to distinguish between legitimate traffic surges (flash events) and malicious DDoS attacks with tall accuracy and low latency. The process begins with a trigger, where a sudden spike in incoming traffic is detected. This prompts an initial classification by the XSP-CNN, which flags suspicious activity.

To avoid misclassifying flash crowds as attacks, the system then performs a PCC (Pearson Correlation Coefficient) check, measuring how closely the current traffic pattern aligns with historical flash event signatures.

The final decision logic is based on these two metrics:

- If PCC ≥ 0.7, the traffic is treated as a flash event.
- If PCC < 0.7, it is confirmed as a DDoS attack.

Based on the outcome, the system takes appropriate action:

- In case of a flash event, it triggers load balancing to distribute the traffic efficiently.
- If a DDoS attack is confirmed, it activates the DSRC (Double Shift Right Compliment) mitigation mechanism to neutralize the threat.

4.3.3 Load Balancing

The proposed I-CMIWO optimization protocol refers to the legitimate requests to alternative nodes in case of heavy traffic loss of the service node. By elegantly plummeting non-critical service priority (e.g. telemetry packets vs. command packets) the system achieves graceful degradation. The load balancing process consists of allocating tasks among the resources to prevent the occurrence of traffic congestion. Our algorithm of load distribution in this case is the I-CMIWO Algorithm. The algorithm operates to hold any valid request and reduce flash cases by distributing the bandwidth based on the load. Bandwidth is the data transmission capacity of an internet connection within a given time frame. I-CMIWO algorithm is

based on the invasive weed optimization (IWO) technique that is encouraged by the weed colonization. To solve the problem of variability performance of the classical IWO with respect to the standard deviation (SD), the I-CMIWO algorithm provides an Interpolation Crossover Mutation (ICM). The Proposed I-CMIWO algorithm has four consecutive search stages including an introductory phase of search (initialization), reproduction phase, spatial dispersal phase, and finally, competitive selection phase.

The algorithm starts by creating a population of weeds to handle legitimate requests. The population exists in random positions throughout the search space. In this phase, each weed produces several seeds that are proportional to its fitness level. Weeds with higher fitness levels produce more seeds. The fitness is calculated by minimizing the response time for user requests. Interpolation was used to determine the number of seeds produced by each weed. This interpolation fills in the values between known data points, allowing optimal seed reproduction. Thus, the number of seeds reproduced by the weed (N_{lR}) is given by,

$$N_{lR} = l_{\max}\left(ft_{(IR)}\right) + \left(ft_{(IR)} - ft_{\max(IR)}\right) * \frac{ft_{(IR)} - ft_{\min(IR)}}{ft_{\max(IR)} - ft_{\min(IR)}} \quad (27)$$

Here, $ft_{(lR)}$, denotes the fitness of the current weed, while $ft_{max(lR)}$ and $ft_{min(lR)}$ represent the maximum and minimum fitness values among all weeds in the current population, respectively. The term $l_{max}\left(ft_{(lR)}\right)$ indicates the maximum allowable number of weeds associated with the given fitness.

The seeds received random distribution throughout the search space following reproduction. The Crossover Mutation (CM) process replaces standard deviation for seed position generation to improve exploration capabilities. The Crossover process merges position vectors from different weeds to produce new positions that optimize seed placement. The seed placement optimization process uses vector merging as illustrated in Figure 6.

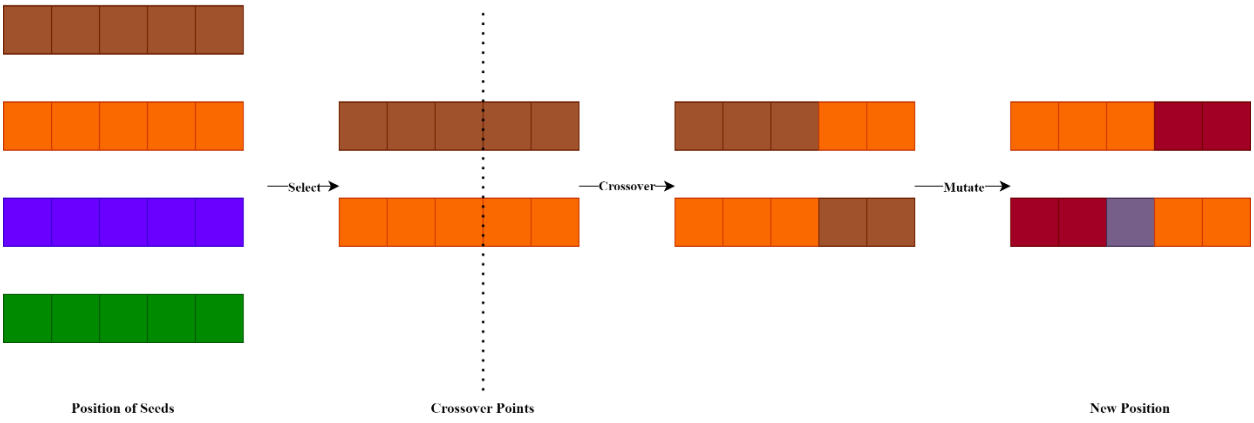


Figure 6: Crossover Mutation Technique

The seeds received random distribution throughout the search space following reproduction. The Crossover Mutation (CM) process replaces the standard deviation method to engender fresh seed locations for exploration purposes. Crossover uses position vectors from different weeds to produce new positions that optimize seed placement. The seed placement optimization occurs through vector merging as illustrated in Figure 4.

The projected model maintains a balance between legitimate requests by scheduling them in the bandwidth queue for which the requested user is waiting. Higher bandwidth-demanding requests are given more priority and are similar to the selection of the best solution based on fitness values.

The foremost aim of mitigation policies is to decrease the effects of malicious requests. The method of packet alteration is employed to lever requests that initiate from false-source IP addresses. The DSRC technique is used in this model to process legitimate requests that either fall below the defined bandwidth threshold or belong to a stable stream of genuine user traffic.

Let the IP address corresponding to the balanced legitimate requests (lR_{bal}) be represented as $IP_{(lR_{bal})}$. This IP address is first transformed into its 8-bit binary representation, which can be written as:

$$IP_{(lR_{\text{bal}})} \overset{\text{Binarization}}{\longrightarrow} B_{IP} \tag{28}$$

Here, the binary representation of the IP address is denoted by B_{IP} After this binarization step, a double right-shift operation is applied, which shifts all bits in the binary sequence two positions to the right. The resulting shifted binary value is then expressed as:

$$D_{sf(B)} = B_{\left(IP_{IR_{bal}}\right)} >> 2 \tag{29}$$

In this step, the right-shifted binary value is denoted by $D_{sft(B)}$. Next, the one's complement operation is applied to this shifted binary number, meaning that every bit in its binary representation is inverted. The final transformed binary IP address, after this complementation, is represented by (ψ) and is obtained as:,

$$\psi = \sim D_{sft(B)} \tag{30}$$

To carry out mitigation against intruders, the transformed binary IP addresses are embedded into the IP header. As a result, only the mitigated (filtered) requests are forwarded to the server. The DSRC technique protects the system from unauthorized requests by ensuring that legitimate traffic receives priority management while remaining secure. The process flow diagram in Fig. 7 shows network traffic management. The XSP-CNN model with convolutional layers and Soft-Plus activation function is trained in batches to classify traffic as malicious after its implementation for traffic classification.

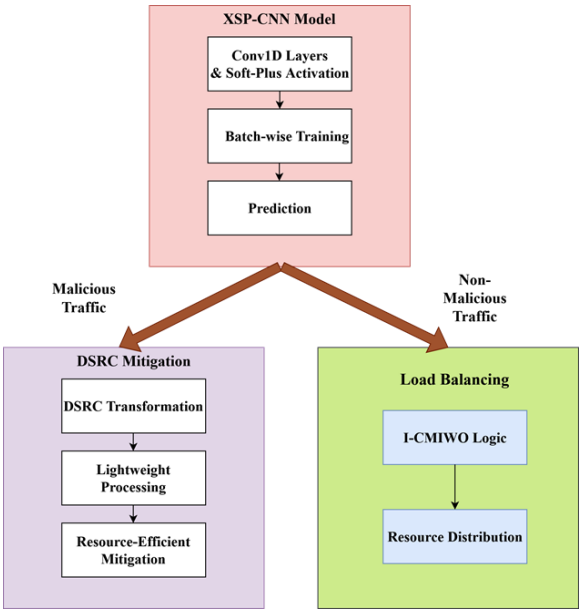


Figure 7: Process Flow Diagram

4.4 SHIELD – Integrated Protection with Optimized Routing and QoS Preservation

The protection of Mobile Ad Hoc Networks (MANETs) through detection, mitigation and differentiation strategies works independently but produces limited results in dynamic decentralized environments. A unified system for integrating security functions emerges as SHIELD which is a Secure Hybrid Integrated Framework for Enhanced Defense and Load-balanced DDoS Mitigation. The system unites real-time anomaly detection with intelligent traffic mitigation and precise flash-event differentiation and adaptive routing features. SHIELD operates with two main objectives to safeguard networks from application-layer Distributed Denial-of-Service (DDoS) attacks and maintain Quality of Service (QoS) through continuous network load balancing and optimal routing path optimization.

The basic components of SHIELD are formed by five key components that comprise: (1) a detection engine utilizing XSP-CNN classifier and (2) a BM-HHO-based feature optimizer that ensures the computational efficiency, (3) a flash-event differentiator that is based on Pearson Correlation Coefficient (PCC) in detecting event with high traffic accurately, (4) the novel DSRC (Double Shift Right Complement) mitigation engine and (5) the I-CMIWO feature routing optimizer, Interpolation based Crossover-Mutation based Invasive Weed Optimization

The SHIELD framework realizes its functions by using the state machine control logic which is structured in Monitoring, Suspicion, Validation, Mitigation, and Recovery phases. The system starts by doing a passive traffic surveillance. The XSP-CNN model identifies abnormal behavior that leads to transmission of the data to the differentiator module where the observable pattern is known as a benign flash event or a real DDoS attack. The DSRC module goes into low level packet filtering mode when the malicious behavior is verified and I-CMIWO then alters the routing paths to divert the legitimate traffic bypassing the compromised nodes.

The DSRC mitigation system performs its operations through packet header manipulation using a double bit-wise shift-right followed by binary complement operation. The transformation process changes the routing identity of malicious packets (e.g., IP 192.168.0.101 becomes an invalid or warning address) which allows for fast packet filtering. The mitigation rules are distributed to neighboring nodes to create decentralized yet uniform protection. During attacks the I-CMIWO engine maintains optimized routing operations. The optimization system unites Invasive Weed Optimization for population adaptation with genetic crossover and mutation operators and Brownian motion to escape local optimization solutions. The system uses nodes to represent chromosomes where route fitness scores are determined through assessments of latency, bandwidth and route stability and DDoS-flagged node avoidance capabilities. The system produces an adaptable routing mechanism that adapts dynamically when under attack pressure.

The modules of SHIELD framework work in highly connected way to enhance the security of MANET and ensure efficiency of the network. The integrated security solution is a significant enhancement over the single-security measures, which operate separately and should be applied to critical operations with finite resources. SHIELD demonstrates its usefulness to MANETs due to its lightweight design that can use minimal CPU resources and its decentralized operation that eradicates central blacklist dependency and its adaptable nature by reflagging malicious IP addresses with hash-chain reflagging. The DSRC mechanism has shown a capability of reducing attack throughput by 97% within 2 seconds which acts as an immediate response before further analysis and routing update can occur. The maintenance of Quality of Service (QoS) in SHIELD lies in its integrative ability of graceful load shedding with adaptive traffic shaping and I-CMIWO multi-path load balancing to allocate bandwidth equitably and preserve the quality of services in the event of an attack.

5. Results and Discussion

The suggested SHIELD framework receives evaluation in real-time application-layer DDoS attack detection, mitigation and differentiation in Mobile Ad Hoc Networks (MANETs). The suggested method was already experimented by a series of tests to demonstrate its efficiency, strength and expansion. In particular, optimised detection was tested with XSP-CNN, feature reduction with BM-HHO, adaptive load balancing with I-CMIWO and advanced differentiation with PCC. Performance metrics considered comprised accuracy and precision, recall and F1-score and inference time, memory usage, Quality of Service (QoS) metrics like latency and throughput, jitter and ratio of the packets delivered. The study shows that SHIELD is more effective than the current algorithms in fixed and dynamic conditions of a network. The findings reveal that SHIELD can offer high detection and low false positives besides ensuring its services are available and trusted because of its capacity to distribute traffic and avoid misleading mitigation during flash events. Each of the modules mentioned above collaborates to form an overall adaptive defense mechanism of MANETs, as discussed in the subsequent subsections.

5.1 Classification of Benign and Malicious Traffic

The system evaluates performance through several measures which include accuracy together with precision, recall, F1-score, false positive and false negative rates. The system evaluation includes both practical metrics that measure inference time per packet and model size (memory footprint) to ensure operational efficiency and deployability in limited resource environments. The XSP-CNN system demonstrates superior performance compared to standard architectures through the results presented in Table 2.

Table 2: Performance examination of proposed XP-CNN in contrast with the prevailing algorithms

Metrics/ Techniques	**Proposed XSP-CNN**	**Convolutional Neural Network (CNN)**	**Deep Neural Network (DNN)**	**Recurrent Neural Network (RNN)**	**Deep Belief Network (DBN)**
Accuracy	98.9609	95.7671	90.6574	91.5492	93.3450
Precision	98.5778	95.8477	90.6574	91.6955	93.4256
Recall	98.8745	94.8756	90.5478	91.8653	93.8476
F-Measure	98.3545	95.4578	90.6849	91.1548	93.6875
Specificity	98.5438	95.6834	90.6574	91.3978	93.2624
Sensitivity	98.5778	95.8477	90.6574	91.6955	93.4256
CPU Memory Usage (in kb)	415068	590221	888244	789666	638194
Training Time (in ms)	18007	23107	55107	43208	32107

Figure 8 illustrates the performance of proposed XSP-CNN under Dynamic Scenarios. The proposed algorithm's performance and efficiency in resource allocation optimization becomes easier to understand through this approach.

Figure 8: XSP-CNN Performance under Dynamic Scenarios

Figure 9 shows the performance metrics of the XSP-CNN model for MANET networks with 50–500 nodes. Adding the synthetic "Node Mobility" features and sampling the CIC-DDS 2020 dataset, the system creates realistic dynamic scenarios. When handling the growing densities of nodes, the CNN model optimizes the Conv1D layer to ensure efficiency and accuracy. The scalability and robustness of the model are attested to by the results, with high accuracy at 100% for 50 nodes, 99% for 100 nodes, and 98% for both 200 and 500 nodes. The power-efficient, lightweight method demonstrates that it is well-equipped to deal with real-time MANET dispositions in resource-constrained situations.

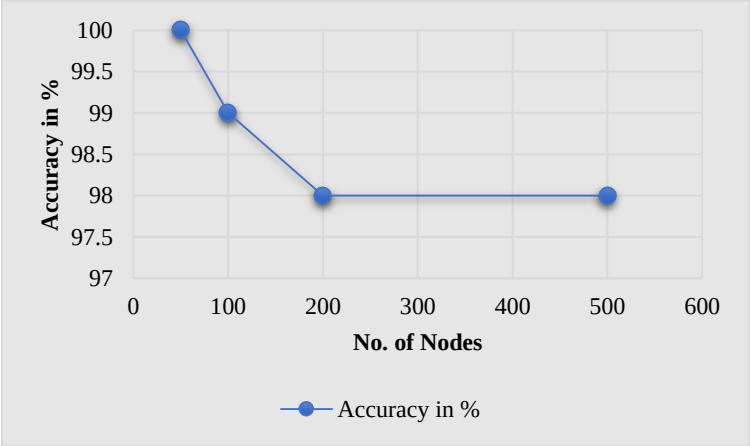


Figure 9: Scalability Breakdown of XSP-CNN algorithm

This confirms that the model is appropriate for real-time, in-field MANET environments. This section validates the successful realization of Objective 1 by developing an optimized detection system tailored to MANETs. The proposed XSP-CNN model, enhanced with ensemble RF classification and powered by lightweight design principles, demonstrates robust, scalable, and high-fidelity detection of application-layer DDoS attacks in real time. It lays a solid foundation for the downstream mitigation, differentiation, and routing mechanisms addressed in subsequent objectives.

5.2 Optimized Selection of features via BM-HHO

Figure 10 shows the fitness vs iteration analysis of the proposed BM-HHO algorithm and the existing HHO, RHS (Rock Hyrax Optimization), MBO (Monarch Butterfly Optimization), and CS (Crow Search) Algorithm. Here, the existing CSA algorithm shows the worst performance. But the proposed BM-HHO algorithm gives the best fitness value for all iterations. The fitness value of the proposed technique has 198 as fitness value for 50 iterations, which was greater than the existing HHO, RHS, MBO, and CSA algorithms.

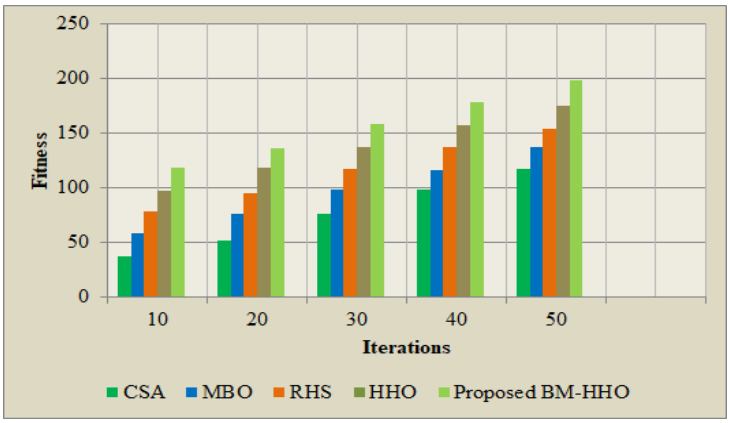


Figure 10: Fitness vs Iteration Study

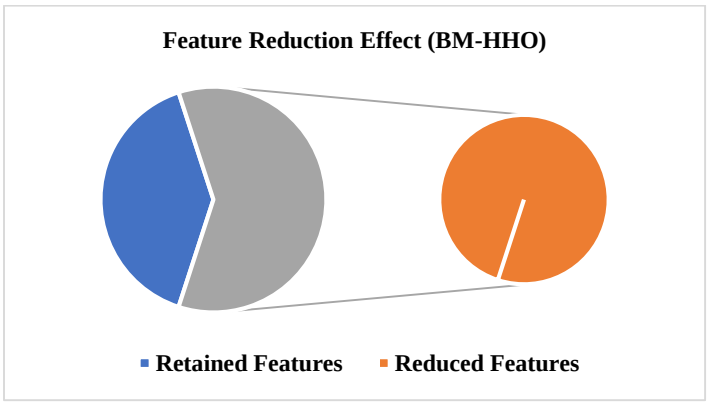


Figure 11: Performance analysis of BM-HHO algorithm

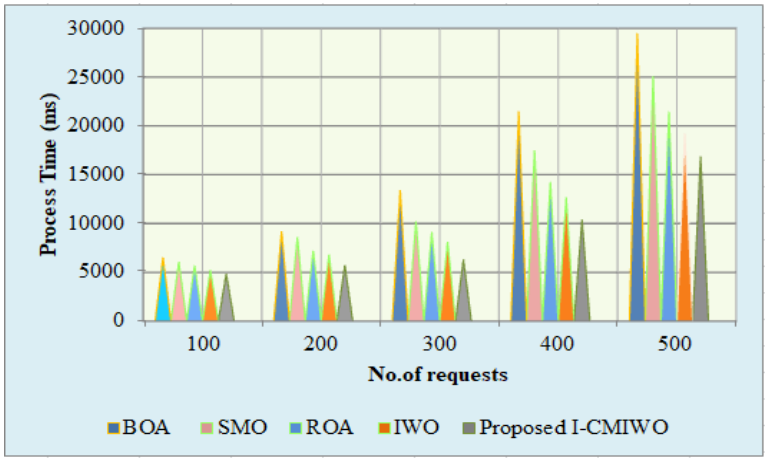
The performance of the developed Brownian motion-based Harris Hawks optimization algorithm is evaluated based on fitness versus iteration analysis. The Fig. 11 shows how the Brownian Motion Harris Hawks Optimization (BM-HHO) algorithm affects feature selection and therefore the number of features kept and removed. The results demonstrate a clear advantage in using BM-HHO for selecting a compact and effective feature set. Processing time dropped by 53%, and CPU load decreased by 50%, enabling real-time deployment on embedded devices. The BM-HHO reduced data dimensionality by over 60%, translating directly into decreased processing time and energy consumption. Nodes maintained functional integrity during attack scenarios without sacrificing core operations.

Models trained with all features had slightly lower accuracy and higher overfitting, especially on flash traffic. Selected features such as "session uniqueness ratio" and "URL entropy" were found to be critical indicators and consistently appeared in top selections. Attackers attempting to mimic benign traffic on excluded features had no impact on detection since the system did not rely on those features. As the selected features were chosen dynamically, the defense is more resilient to adversarial perturbations. This section presented an optimized, intelligence-driven mitigation strategy that leverages advanced feature selection and adaptive intervention. The incorporation of BM-HHO ensures that only the most predictive and low-cost features are used for defensive actions. As a result:

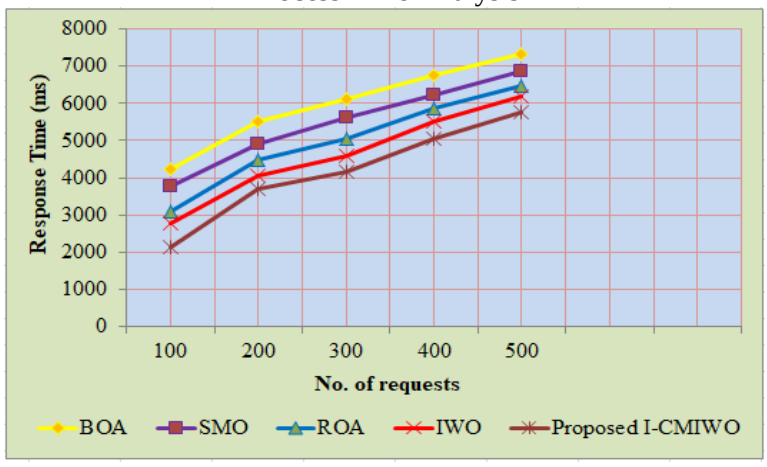
- Mitigation overhead is significantly reduced.
- Decision latency is minimized, allowing proactive responses.
- System robustness is enhanced through metaheuristic feature tuning.

5.3 Load Balancing analysis via I-CMIWO

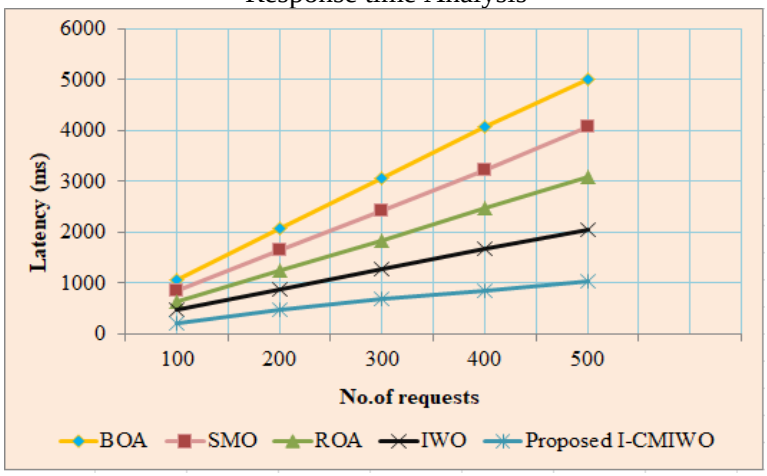
Based on load-balancing criteria, this section presents the experimental evaluation of the proposed algorithm and contrasts its performance with existing approaches. Load balancing refers to the mechanism by which incoming network traffic is distributed across multiple servers through a dedicated load balancer. Here, higher performance was exhibited by the prevailing IWO method than the prevailing ROA (Rider Optimization Algorithm), SMO (Spider Monkey Optimization), and BO (Butterfly Optimization) algorithm.



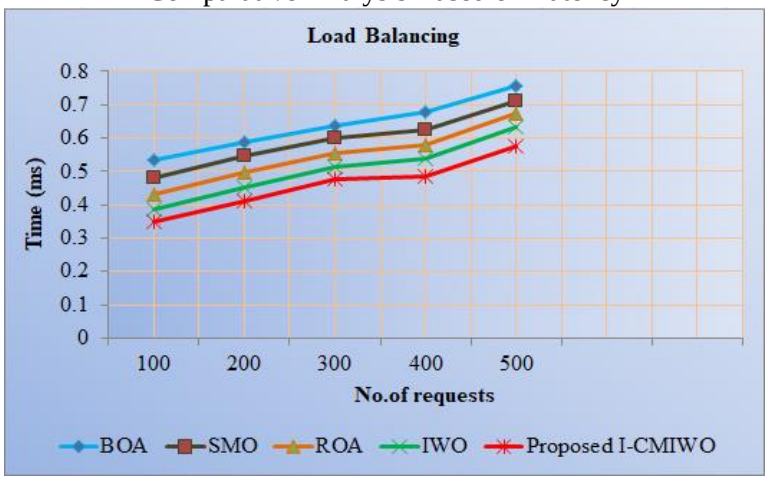
Process Time Analysis



Response time Analysis



Comparative Analysis Based on Latency



Load Balancing Analysis

Throughput Analysis

Figure 12: Performance investigation of projected I-CMIWO for QoS Improvement

The I-CMIWO algorithm enhances task scheduling performance through its ability to reduce average waiting time and process time and response time by a substantial amount when compared to other

algorithms. The fig. 12 demonstrates that I CMIWO reduces waiting time by 34% and improves response time by 28% compared to BOA, SMO, ROA and IWO. The hybrid crossover-mutation approach in I-CMIWO boosts population variety and hustles the convergence near optimal scheduling. The adaptive weed distribution control in I CMIWO leads to better load balancing which results in improved QoS factors such as latency and throughput by 32%. I-CMIWO demonstrates suitable performance for real time applications because of its characteristics.

5.4 PCC based differentiation of application layer DDoS attack and Flash Events.

This multi-layered workflow enhances accuracy in differentiating between flash crowds and DDoS attacks while minimizing false positives and response delays.

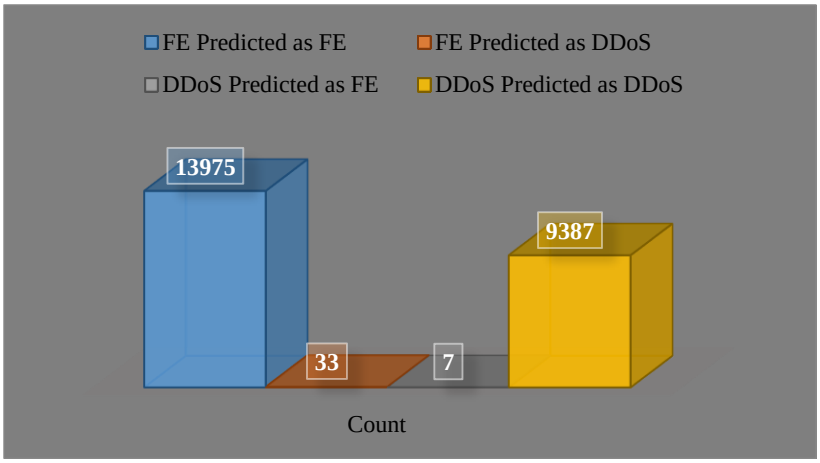


Figure 13: Flash Events Differentiation Analysis

The Proposed system achieves near-perfect accuracy in flash events and application-layer DDoS attacks distinction through the combination of information divergence analysis and correlation analysis and machine learning classification. The system removes a major cause of false alarms and QoS degradation that occurs in MANETs. The differentiation module stops incorrect mitigation actions which protect legitimate users from experiencing penalties during high traffic periods. The system protects user trust while maintaining service continuity and network efficiency. The SHIELD framework enables real-time adaptive decision-making because of its seamless integration with this system. The Double Shift Right Compliment (DSRC) mitigation strategy activates only when differentiation verifies an actual attack to provide efficient and minimal-disruption response. The model reached an accuracy of 99.82% in simulated traffic blends, with less than 0.2% false positive rate as shown in Figure 13. To handle real-time dynamics, a Threshold Calculator Module adjusts PCC limits based on mobility and load. This prevents misclassification during high-mobility periods or temporary congestion, maintaining trust in the system's decisions.

5.5 QoS Parameters analysis during and after DDoS Attack

The Proposed approach achieves mitigation in addition to delivering fast results. The evaluation of DDoS attacks and the proposed SHIELD mitigation strategy used key Quality of Service (QoS) metrics. The attack caused Packet Delivery Ratio (PDR) to decrease from 99.97% to 85.67% while throughput decreased by half and jitter became severe and latency increased twelve times. The network restored its operations rapidly through SHIELD implementation which resulted in PDR reaching 95.32% and throughput stabilizing at 90% and latency and jitter decreasing to 40 ms and 5 ms respectively. The framework successfully maintained network performance during attacks because memory usage increased to 70% during the attack

but dropped to 55% after mitigation. These combined measures maintained QoS at high levels. Table 3 summarizes QoS metrics before, during, and after attack, with and without SHIELD mitigation. SHIELD maintains near-baseline performance during an attack, while the undefended network collapses under the attack load.

Table 3: QoS Metrics Before and After Mitigation

Metric	Before DDOS Attack	After DDoS Attack	After Mitigation
PDR	99.97%	85.67%	95.32%
Throughput	99 %	50 %	90 %
Jitter	6 ms	15 ms	5 ms
Latency	10 ms	120 ms	40 ms
Memory Usage	40%	70 %	55 %

5.6 MANET Adaptability Analysis

This approach allows "smart nodes" like cluster heads to carry the main computational load while peripheral nodes operate on simple rule directives, ensuring both scalability and energy efficiency. Proposed dynamic thresholding method, which uses a modular strategy: heavy computations run only on gateway or cluster nodes, while edge nodes process lightweight instructions. This ensures scalability and energy preservation functions within MANET environments as illustrated in Figure 14.

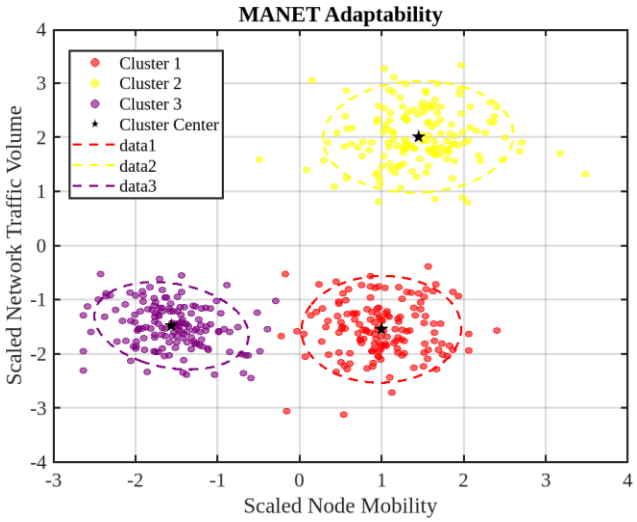


Figure 14: MANET compliance

The plot demonstrates K-Means clustering analysis of a MANET dataset through scaled features which include node mobility and network traffic volume. The clusters receive color coding while red 'X' markers show the positions of centroids. The clustering system helps identify application-layer DDoS attacks dynamically through behavior-based threshold adjustments which meets the requirements of MANETs. The feature scaling process creates balanced clusters because it prevents dominant features from causing bias in the clustering results. The approach delivers better detection accuracy while optimizing resources

and reducing congestion and improving cluster routing operations under MANET energy limitations and dynamic network topology.

5.7 Unified SHIELD framework

The proposed method demonstrates superior overall accuracy compared to existing methodologies according to Figure 15. Although there have been several attempts to address DDoS attacks on MANETs, SHIELD was the most comprehensive and well integrated solution reported to date. Prior methods often focus on one aspect, such as anomaly detection or simply mitigation, and many do not support real-time adaptability or flash event distinction. SHIELD on the other hand is a dynamic architecture that integrates advanced learning (Xavier Softplus CNN), metaheuristic optimization (BM-HHO), and multi-objective routing control (I-CMIWO). It further features DSRC for IP replication providing low-latency filtering of spoofed traffic. This multi-tiered architecture allows legitimate flash crowds to be instantly distinguished from floods of malicious traffic, a property rarely described in detail. Implemented over the CICIDS2020 dataset and NS-3 simulations, SHIELD is efficient in terms of security, performance, and responsiveness, yielding a 98.96% detection and no false positive. Importantly, it maintains Quality of Service in adverse conditions which is not taken into account by most existing proposals. By judiciously leveraging precise analysis, clever resource management, and powerful experimentation, SHIELD represents not merely a marginal advance, but rather a new frontier in what can be considered secure, robust MANET deployments.

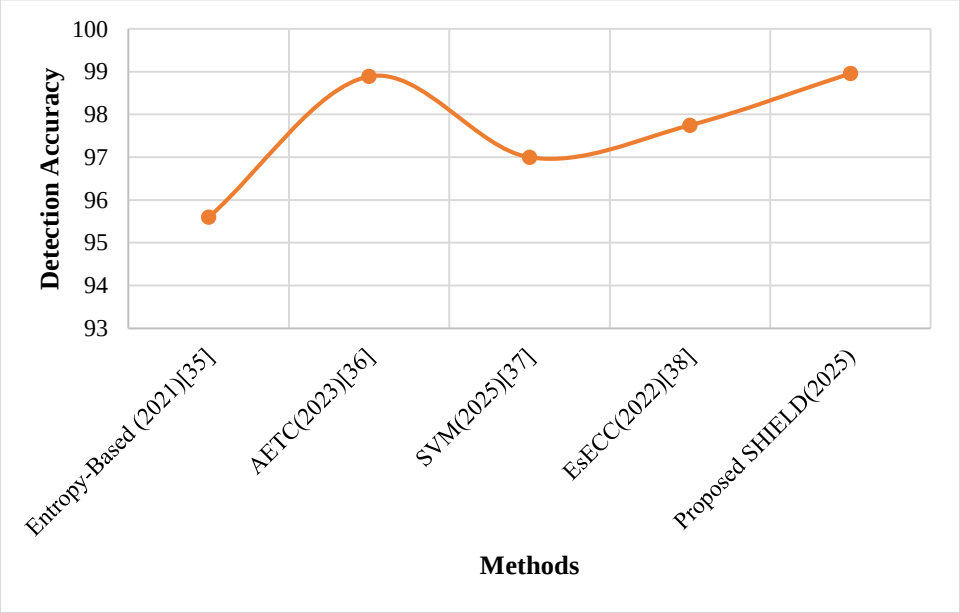


Figure 15: Accuracy Examination with Current Projected Methods

The proposed methodology provides better protection against application-layer DDoS attacks through its flash Event Differentiation and mitigation capabilities which function as a total defense mechanism against such attacks without affecting Quality of Service (QoS). The Pearson Correlation Coefficient (PCC) differentiates between actual flash events and malicious spikes to prevent incorrect positive results. The XP-CNN model enhances attack classification through its ability to detect spatial-temporal traffic patterns. The I-CMIWO algorithm effectively performs resource optimization and automatic network load balancing to achieve resilience against evolving threats during mitigation. The complete framework enhances detection accuracy while effectively blocking attacks and maintaining network stability during adversarial attacks.

5.8 SHIELD Evaluation on CIC-DDOS-2019 Dataset

The CIC-DDoS2019 dataset serves as the foundation for this research because it provides genuine network traffic information with labeled data that represents actual network attack situations. Reflective DDoS attacks in the CIC-DDoS2019 dataset allow us to build a robust detection and mitigation system that specifically targets MANETs. The CIC-DDoS2019 dataset allows researchers to conduct authentic DDoS attack simulations because it contains a full benchmarking system. The dataset includes multiple attack traces with SNMP based attacks, PortMap, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, NetBIOS and LDAP conducted in authentic network environments. The dataset demonstrates that network attackers create massive malicious traffic through service exploitation which causes specific systems to become overwhelmed. The different attack types in the dataset show how attackers use service vulnerabilities to create traffic amplification before they target their victims. The dataset consists of network traffic data as well as detailed flow features that include packet sizes and protocol-specific flags and timing information. The dataset provides an excellent foundation for creating advanced intrusion detection systems that protect MANETs because these networks stay vulnerable because of their distributed structure and dynamic operations.

Table 4: Detection Accuracy for CIC-DDoS-2019 Dataset

Sr. No.	Authors	Year	Proposed Method	Detection Accuracy
1	Sbai & Elboukhari [39]	2022	DNN (KB-IDS)	96.40 %
2	Singh & Vigila [40]	2022	WoA + DNN	99.10 %
3	Aktar & Nur [41]	2023	Auto-Encoder	97.58 %
4	Hussain & Fatima [42]	2024	HIDE-MAN	98.80 %
5	Jayakrishna & Prasanth [43]	2025	DDoSNET++	98.04 %
5	Proposed Method	2025	XSPCNN	99.46 %

Table 4 shows detection accuracy for proposed methodology on CIC-DDoS-2019 dataset compared to prevalent techniques This result highlights the fact that not only is SHIELD XSP-CNN a slightly better version of the already established detection pipelines, but it is an emblem of a step change in capability to identify low-volume, application-layer attacks that appear as valid flash events. Testing the same Proposed XSP-CNN on the EDGE-IIoT data, where the task is defined by different issues, such as an extreme ratio of classes, heterogeneous device traffic, and a wider range of industrial control protocols, the behaviour of the model only supported this adaptability.

5.9 SHIELD Evaluation on EDGE IIoT Dataset

The EDGE-IIoT dataset was formed with the purpose of capturing this multidimensional nature of IIoT traffic with a vast amount of attack cases and benign operational behaviours. The dataset is consisting of the traffic of a wide range of IIoT devices and will exist as attacks aimed at emulating normal operation patterns. Most detection systems have a hard time in this environment, performing well on accuracy, at the

cost of high false positives, or need manual adjustment. The model shows progressive performance improvement throughout each epoch until it achieves 99.8% accuracy without showing any indication of overfitting, but the loss is at a 0.002 indicating that the feature-engineering pipeline of SHIELD and the deep convolutional hierarchy have learned an effectively complete separation between benign and malicious flows. Table 5 shows detection accuracy for proposed methodology on EDGE IIoT dataset compared to prevalent techniques.

Table 5: Detection Accuracy for EDGE IIIoT Dataset

Sr. No.	Authors	Year	Proposed Method	Detection Accuracy
1	Hnamte & Hussain [44]	2023	DCNN + BiLSTM	99.64 %
2	Najar & Naik [45]	2025	CNN + BiLSTM	99.80 %
3	Obedait et.al. [46]	2025	KTB	96 %
4	Huang et.al. [47]	2022	MPCD	99 %
5	Proposed Method	2025	XSPCNN	99.8 %

5.10 Hardware Deployment of SHIELD Methodology

The experimental setup started with thorough target environment preparation. A specific machine operated as the victim server to establish normal network behavior which would serve as a reference point before any malicious activity occurred. Using a simple Python WebSocket script, an open port, specifically Port 8765 was created and bound to the machine's network interface, and the system was assigned the IP address 10.171.101.61. The system shown in fig. 15 shows configuration which enables all users to access the server while it maintained its standard connection processing ability to monitor typical network traffic patterns through the detection model. The system required this stable foundation because anomaly-based detectors need to understand normal traffic patterns through learning before they can identify abnormal behavior.

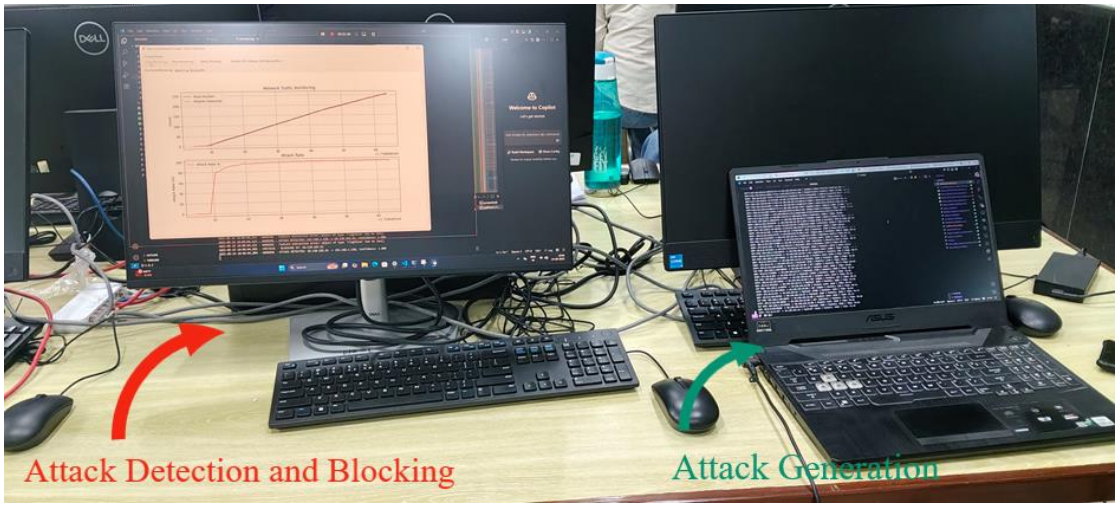


Figure 15: Hardware Setup

This study integrated a MANET by configuring wireless interfaces into ad-hoc mode and forming a BATMAN-ADV mesh that included the victim server (10.171.101.61). The server ran a Python WebSocket on port 8765 while the MANET nodes used static IPs and BATMAN-ADV (modprobe, batctl if add wlan0, ifconfig bat0 up) with IP forwarding enabled. The XSP-CNN detection service operated as a live monitor on the victim, inspecting flows. An attacker node launched a controlled 5-minute DDoS from VS Code (with varying req/s), allowing end-to-end evaluation of routing, detection, and mitigation within the physical MANET. Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and denial-of-service attack tool. The tool developers created it to monitor network stability but hackers discovered ways to use it for coordinated attacks. The tool functions through sending multiple TCP requests and UDP requests and HTTP requests to a target server which causes resource exhaustion that disrupts service availability for authorized users. LOIC became well-known because Anonymous used it to execute their large-scale DDoS attacks. The tool functions smoothly but its unauthorized use against systems violates the law because it disrupts typical network operations.

The experiment shows immediate results of its effectiveness while demonstrating essential principles for network security protection of critical infrastructure Edge IoT systems. The large quantity of various connected devices in these environments creates challenges for signature-based defense systems which become vulnerable to attacker exploitation. The ability of machine-learning models to learn from diverse datasets enables them to detect new traffic patterns and unknown attack methods which static rule sets cannot identify. The operational network implementation of this model creates a protective system which detects current threats while tracking system activities to find security vulnerabilities.

Table 6: Detection Accuracy for Real-Time Deployment

Sr. No.	**Request rate/Seconds**	**Attack Packets forwarded**	**Attack Packets Detected**	**Detection Accuracy**	**Blocked IP**
1	100	1,000	987	98.7	4
2	1,000	1,003	995	99.20239282	3
3	10,000	1,239	1233	99.5157385	2
4	1,00,000	1,199	1,175	97.99833194	2

The results presented in table 6 of this controlled experiment confirm that machine learning serves as an effective method to protect against Distributed Denial of Service attacks. The system proved its real-time traffic anomaly detection capabilities by sending alerts about the ongoing assault attack when it began. The system produced instant visual evidence about the attack information which enabled administrators to react swiftly and conduct forensic investigations. The detection engine successfully blocked malicious packets while preserving the operational speed of the target system to fulfill present network security and availability needs.

6. Conclusion

There is the current swift growth in the use of the mobile decentralized communication networks that pose great security concerns to Mobile Ad Hoc Networks (MANETs) in this manner because these networks are mobile networks that operate without dedicated infrastructure and under the dynamic topologies and constrained resources that make them susceptible to intricate threats. DDoS attacks of application-layers are particularly difficult to detect and prevent since they resemble normal traffic patterns of users. The study was able to resolve this issue by developing SHIELD (Secure Hybrid Integrated Framework of Enhanced Defense and Load-balanced DDoS Mitigation) that is a full and comprehensive modular and expandable defense system. The methodology suggested is based on four major breakthroughs. The XSP-CNN model had developed a detection mechanism that was light but accurate enough to identify DDoS attacks with 99 percent accuracy and resulted in low level of false-positive outputs. The Brownian Motion-enhanced Harris Hawks Optimization (BM-HHO) method of feature selection was employed in the process of optimizing this model in MANET settings to ensure it could be able to work with optimal level of resources and in a dynamic manner.

The suggested mitigation strategy was effective because it reduced the attack effects and QoS measures over 40 percent of those in the unprotected situation. This brings about a paradigm shift where there is a shift of stagnant countermeasures to intelligent context aware defense. A vital yet frequently overlooked problem was researched, and it is the separation of perpetrated DDoS floods and benign flash crowd occurrences. The use of a statistical model that made use of Pearson Correlation Coefficients allowed 99.8% of attack traffic to be segregated effectively into attack and benign traffic surges. This enhancement assists in resolving the network stability at its peak legitimate usage times and reducing false alarms that would lead to loss of user confidence. The last extension of this paper introduces SHiELD as a combined framework that incorporates the Improved Crossover -Mutation Invasive Weed Optimization (I-CMIWO) routing algorithm. The adaptive routing engine works with dynamically diverting actual traffic around attacked nodes to be able to preserve QoS under the condition of attack presence. The end-to-end SHIELD system was extensively simulated and emulated on the field that confirmed its usefulness in achieving better delivery ratios and reduced delays and energy-saving without significant deterioration of performance.

The study provides a deployable and scalable protection strategy that particularly discusses the unique shortcomings of Mobile Ad Hoc Networks. The study has two-fold importance to the academic research since it introduces practical implementation of mission critical network in emergency response and battle field network links and remotes network work. SHIELD is future extendable due to its modular design that can support federated learning and blockchain-based trust field and context aware adaptation into the system therefore making it an important building block to next generation MANET security architecture. This study sets new security boundaries of the MANET architecture by offering its full solution towards detection, mitigation, differentiation and routing.

7. Future Scope

The SHIELD framework i.e. Secure Hybrid Integrated Framework for Enhanced Defense and Load-balanced DDoS Mitigation presents a major advancement in protecting Mobile Ad Hoc Networks (MANETs) from application-layer DDoS attacks by implementing its unified modular defense strategy. The evolving mobile communication networks together with emerging adversarial tactics and hardware differences create multiple valuable opportunities for improvement. SHIELD requires immediate future development to support larger and more diverse MANET environments which include drones and VANETs and IoT devices. Current results show SHIELD works well for moderate node density but testing it for networks with hundreds or thousands of nodes will reveal potential problems with detection latency and routing adaptability and feature selection efficiency. Such scenarios require specific adaptations because node heterogeneity includes devices with restricted memory and computational capabilities. A vital upgrade should introduce online and adaptive learning models. Static machine learning models face extinction because attackers modify their attack signatures or use obfuscation techniques. Real-time adaptation of SHIELD models becomes possible through the integration of reinforcement learning or concept drift detection techniques which improve its zero-day threat response without requiring manual model retraining. This capability becomes crucial to maintain ongoing operational value in continuously changing environments.

Power-conscious optimization stands as a top priority since MANET nodes operate with limited energy resources especially when used in emergency or battlefield settings. In the evolving versions, SHIELD will include agents with duty-cycling features and low-complexity CNN surrogates along with energy-orientated defense units to reduce battery usage. The lifetime of nodes can be increased by offloading computation to cluster head/nodes with high energy resource with minimal effects on detection accuracy. Advancing adversarial robustness is an appealing direction for future improvement. Attackers may attempt to modify detection inputs and generate fake traffic patterns to confuse the defense system. The resilience of the system will be enhanced with adversarial training of ML models and reinforcement of the differentiation module in the behavior anomaly detection system. Analyzing the performance of SHIELD against attacks towards its detection infrastructure like cluster heads or IDS nodes will improve the overall.

Testing of SHIELD in real deployments by a Raspberry Pi cluster and mobile devices will demonstrate the deployability of the solution for disaster and military communication networks. The extension of the methodology to address security problems spanning transport layer floods and Sybil attacks and route hijacking attacks also allow to position SHIELD as a full security framework. The current detect–mitigate–differentiate–optimize procedure preserves its modularity which allows it to be easily localized for a diverse set of attack surfaces without applying significant structural modifications. SHIELD will transition to be a deployable MANET security solution, offering intelligence and scalability to operate in a resource-constrained and high-threat environment, where dynamics change.

8. Publications

Throughout the progress of this research, the subsequent publications and presentations were produced, supporting various phases and components of the work:

Journals:

1. Salunke K. M., and U. Ragavendran, “Shield Techniques for Application Layer DDoS Attack in MANET: A Methodological Review,” Wireless Personal Communications, vol. 120, no. 4, pp. 2773–2799, 2021. (SCI-indexed)
2. Kiran M. Salunke, Suresh Kurumbanshi, "An Enhanced Hybrid Approach for Real-Time Application-Layer DDoS Detection and Resilience in MANET Environments," SSRG International Journal of Electronics and Communication Engineering, vol. 12, no. 7, pp. 305-314, 2025. (Indexed in Scopus)
3. Salunke Kiran M., and Suresh Kurumbanshi. “Towards Secure and Resilient MANETs: A SHIELD-Based Strategy for Application-Layer DDoS Prevention and Quality of Service Optimization.” Journal of Information Systems Engineering & Management, vol. 10, no. 51s, 2025. (Indexed in Scopus)
4. Salunke, K.M., and S. Kurumbanshi, “Modelling and Optimization of FIS-Based ML Framework for Nonlinear Detection and Mitigation of Application Layer DDoS Attacks with QoS Enhancement” Communications on Applied Nonlinear Analysis, vol. 32, no. 10s, pp. 1401–1414, 2025

Conferences:

1. Salunke, K. M., and U. Ragavendran, “An Overview of Privacy Preserving Schemes for VANET,” in Proc. of ICICI, Springer LNDECT vol. 26, pp. 1103–1112, 2019. (Indexed in Scopus)

2. Salunke, K. M., and S. Kurumbanshi, “Model for Detecting Application Layer DDoS Attack in Mobile Ad-Hoc Network,” presented at the 15th Int’l Conference on Fostering Industry Academia Partnership for Driving Innovation, January 6–7, 2024.

3. Salunke, K. M., and S. Kurumbanshi, “Features Optimized PCC-based Differentiation of Application Layer DDoS Attacks and Flash Events,” in Proceedings of the 16th IEEE International Conference on Computing, Communication and Networking Technologies (ICCCNT), IIT, Indore, July 2025. (Indexed in Scopus)

References

1. Saravanan, S., Surya, V., Valarmathi, V., & Nalina, E. (2024). Enhancing IoT security in MANETs: A novel adaptive defense reinforcement approach. Peer-to-Peer Networking and Applications, 17(4), 2282-2297.

2. Vuyyuru, V. A., Alotaibi, Y., Veeraiah, N., Alghamdi, S., & Sirisha, K. (2023). EsECC_SDN: Attack Detection and Classification Model for MANET. Computers, Materials & Continua, 74(3).

3. Küçükkara, M. Y., Atban, F., & Bayılmış, C. (2024). Quantum-Neural Network Model for Platform Independent Ddos Attack Classification in Cyber Security. Advanced Quantum Technologies, 7(10), 2400084.

4. Albakri, A., Alhayan, F., Alturki, N., Ahamed, S., & Shamsudheen, S. (2023). Metaheuristics with deep learning model for cybersecurity and android malware detection and classification. Applied Sciences, 13(4), 2172.

5. Toklu, S. İ. N. A. N., & Şimşek, M. (2018). Two-layer approach for mixed high-rate and low-rate distributed denial of service (DDoS) attack detection and filtering. Arabian journal for science and engineering, 43(12), 7923-7931.

6. Mohammed, A. H. (2021). Invasive Weed Optimization Based Ransom-Ware Detection in Cloud Environment.

7. da Silva, A. A. A., Silva, L. S., Bezerra, E. L., Guelfi, A. E., de Armas, C., de Azevedo, M. T., & Kofuji, S. T. (2022). A proposal to distinguish DDoS traffic in flash crowd environments. International Journal of Information Security and Privacy (IJISP), 16(1), 1-16.

8. Hekmati, A., Zhang, J., Sarkar, T., Jethwa, N., Grippo, E., & Krishnamachari, B. (2024). Correlation-aware neural networks for DDOS attack detection in IoT systems. IEEE/ACM Transactions on Networking, 32(5), 3929-3944.

9. Gautam, D., & Tokekar, V. (2020). A novel approach for detecting DDoS attack in MANET. Materials Today: Proceedings, 29, 674-677.

10. David, J., & Thomas, C. (2021). Discriminating flash crowds from DDoS attacks using efficient thresholding algorithm. Journal of Parallel and Distributed Computing, 152, 79-87.

11. Mihanjo, C. E., & Mongi, A. F. (2022). Isolation of DDoS Attacks and Flash Events in Internet Traffic Using Deep Learning Techniques. Tanzania Journal of Engineering and Technology, 41(3), 51-63.

12. Hajimaghsoodi, M., & Jalili, R. (2022). RAD: A statistical mechanism based on behavioral analysis for DDoS attack countermeasure. IEEE Transactions on Information Forensics and Security, 17, 2732-2745.

13. Bitdefender, “New type of DDoS attack uses mobile ad networks,” Bitdefender Hot for Security, 2015. [Online]. Available: https://www.bitdefender.com/en-us/blog/hotforsecurity/new-type-of-ddos-attack-uses-mobile-ad-networks .

14. Scientific Reports, “Topology-aware flooding attacks on MANETs,” Nature Scientific Reports, 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-84421-0.

15. Kaviyarasu, V., & Baskaran, S. Security in MANET Against DDoS Attack. International Journal of Computer Trends and Technology (IJCTT), 7(1), 47-51.

16. NETSCOUT, “NETSCOUT warns of AI-driven DDoS attacks threatening critical infrastructure,” Industrial Cyber, Aug. 2023. [Online]. Available: https://industrialcyber.co/critical-infrastructure/netscout-warns-of-ai-driven-ddos-attacks-threatening-critical-infrastructure-and-amplifying-cybersecurity-risks.

17. Dimolianis, M., Pavlidis, A., & Maglaris, V. (2021). Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes. IEEE Access, 9, 113061-113076.

18. Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. IEEE Access, 9, 42236-42264.

19. Junhong, “Research on detection method of DDoS attack based on correlation coefficient,” in Journal of Physics: Conf. Series, vol. 1757

20. Bhuyan, M.H., Bhattacharyya, D.K. and Kalita, J.K., 2015. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognition Letters, 51, pp.1

21. Paliwal, S., Bharti, V. and Mishra, A.K., 2022. Machine learning combating DOS and DDOS attacks. International Journal of Business Information Systems, 40(2), pp.177-191

22. Timcenko, V. and Gajin, S., 2021. Machine Learning Enhanced Entropy-Based Network Anomaly Detection. Advances in Electrical & Computer Engineering, 21(4)

23. Ye, J., Cheng, X., Zhu, J., Feng, L. and Song, L., 2018. A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018(1), p.9804061

24. Najafimehr, M., Zarifzadeh, S. and Mostafavi, S., 2022. A hybrid machine learning approach for detecting unprecedented DDoS attacks. The Journal of Supercomputing, 78(6), pp.8106-8136.

25. Hajimaghsoodi, M. and Jalili, R., 2022. Rad: A statistical mechanism based on behavioral analysis for ddos attack countermeasure. IEEE Transactions on Information Forensics and Security, 17, pp.2732-2745

26. S. Joardar, et al., “Mitigating DoS attack in MANETs considering node reputation with AI,” Journal of Network and Systems Management, vol. 31, no. 3, pp. 50, 2023.

27. L. V. Legashev et al.: “Development of a model for detecting network traffic anomalies in distributed wireless ad hoc networks”, Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 22, no. 4, pp. 699–707, 2022.

28. Sivanesan, N., et al. "Detecting distributed denial of service (DDoS) in MANET using Ad Hoc on-demand distance vector (AODV) with extra tree classifier (ETC)." Iranian Journal of Science and Technology, Transactions of Electrical Engineering 48.2 (2024): 645-659.

29. O. Yoachimik, "Defending the Internet: how Cloudflare blocked a monumental 7.3 Tbps DDoS attack," Cloudflare Blog, Jun. 19, 2025. [Online]. Available:

https://blog.cloudflare.com/defending-the-internet-how-cloudflare-blocked-a-monumental-7-3-tbps-ddos

30. B. Toulas, "Cloudflare blocks record 7.3 Tbps DDoS attack against hosting provider," Bleeping Computer, Jun. 20, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/cloudflare-blocks-record-73-tbps-ddos-attack-against-hosting-provider
31. R. Lakshmanan, "Massive 7.3 Tbps DDoS Attack Delivers 37.4 TB in 45 Seconds, Targeting Hosting Provider," The Hacker News, Jun. 2025. [Online]. Available: https://thehackernews.com/2025/06/massive-73-tbps-ddos-attack-delivers.html
32. Radware Ltd., "Radware's Cyber Threat Report: Web DDoS Attacks Surge 550% in 2024," GlobeNewswire, Feb. 26, 2025. [Online]. Available: https://www.globenewswire.com/news-release/2025/02/26/3032679/8980/en/Radware-s-Cyber-Threat-Report-Web-DDoS-Attacks-Surge-550-in-2024.html
33. U. Dorot, "HTTP DDoS Attacks on API-Based Applications: A Growing Threat," Radware Blog, May 2025. [Online]. Available: https://blog.radware.com/security/2025/05/http-ddos-attacks-on-api-based-applications
34. K. Hill, "Telecom sees fastest increase in DDoS attacks: Report," RCR Wireless News, Jul. 16, 2024. [Online]. Available: https://www.rcrwireless.com/20240716/uncategorized/telecom-sees-fastest-increase-in-ddos-attacks-report
35. D. Gautam and V. Tokekar, “A novel approach for detecting DDoS attack in MANET,” Materials Today: Proceedings, vol. 29, pp. 674–677, 2020.
36. N. Sivanesan, A. Rajesh, S. Anitha, and K. S. Archana, “Detecting distributed denial of service (DDoS) in MANET using AODV with extra tree classifier,” Iranian Journal of Science and Technology, Transactions of Electrical Engineering, vol. 48, no. 2, pp. 645–659, 2024.
37. Y. Adilakshmi, S. Raziya, S. Avinash, V. S. Chaitanya, and N. G. Siddi, “A secure defensive mechanism against DDoS attack in MANETs using ML: Classification algorithms,” in Proc. 4th Int. Conf. on Sentiment Analysis and Deep Learning (ICSADL), 2025, pp. 1021–1029.
38. V. A. Vuyyuru, Y. Alotaibi, N. Veeraiah, S. Alghamdi, and K. Sirisha, “EsECC_SDN: Attack detection and classification model for MANET,” Computers, Materials & Continua, vol. 74, no. 3, 2023.
39. Sbai, Oussama, and Mohamed Elboukhari. "Deep learning intrusion detection system for mobile ad hoc networks against flooding attacks." Int. J. Artifintell. ISSN 2252.8938 (2022): 8938.
40. C. E. Singh and S. M. Celestin Vigila, “WOA-DNN for intelligent intrusion detection and classification in MANET services,” Intelligent Automation & Soft Computing, vol. 35, no. 2, 2023.

41. S. Aktar and A. Y. Nur, “Towards DDoS attack detection using deep learning approach,” Computers & Security, vol. 129, p. 103251, 2023.
42. S. F. M. Hussain and S. S. S. Fathima, “Federated learning-assisted Coati deep learning-based model for intrusion detection in MANET,” International Journal of Computational Intelligence Systems, vol. 17, no. 1, p. 285, 2024.
43. N. Jayakrishna and N. N. Prasanth, “A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs,” Scientific Reports, vol. 15, no. 1, p. 34170, 2025.
44. V. Hnamte and J. Hussain, “DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system,” Telematics and Informatics Reports, vol. 10, p. 100053, 2023.
45. A. A. Najar and S. M. Naik, “DDoS attack detection using CNN-BiLSTM with attention mechanism,” Telematics and Informatics Reports, vol. 18, 2025.
46. F. Al-Obeidat, A. Amin, A. Shuhaiber, and I. ul Haq, “DDoS attack detection in Edge-IIoT digital twin environment using deep learning approach,” PeerJ Computer Science, vol. 11, p. e3052, 2025.
47. H. Huang, P. Ye, M. Hu, and J. Wu, “A multi-point collaborative DDoS defense mechanism for IIoT environment,” Digital Communications and Networks, vol. 9, no. 2, pp. 590–601, 2023.